E-Jenayah Ancaman Alaf Digital

Oleh

Mohamad Zaki Ibrahim

Projek Penyelidikan bagi memenuhi sebahagian daripada
syarat-syarat untuk Ijazah Sarjana Pengadilan Jenayah

2001/2002

ABSTRAK

Internet boleh dikatakan sebagai inovasi teknologi yang terbesar selepas revolusi industri, hasil dari gabungan teknologi maklumat dan komunikasi serta jalinan rangkaian sistem komputer. Lantaran itu maka lahirlah 'alam' yang dikenali sebagai Internet, yang bersifat 'maya' (virtual) atau disebut sebagai alam siber. Akibatnya, hampir keseluruhan besar struktur politik, ekonomi, sosial dan budaya masyarakat 'dipaksa' menerima arus perubahan sehinggakan mulai mencorakkan semula berbagai amalan dan perlakuan 'baru' manusia pada masakini. Ternyata Internet, yang dihasilkan dari ribuan jalinan sistem rangkaian komputer dan sistem data otomasi (automated data systems) memberi peluang baru yang cukup meluas kepada kita untuk turut serta dalam arus kemajuan digital yang pesat. Tidak ketinggalan juga untuk mereka yang ingin melakukan jenayah dengan mengadaptasi prasarana digital mereka dapat menyempunakan berbagai perlakuan jenayah 'baru' dengan 'mendigital' jenayah tradisi. Golongan ini dikenali sebagai pelaku e-jenayah. Kini dengan kedapatan dan kemudahan komputer dan peralatan elektronik yang canggih didapati seolah-olah begitu mudah untuk seseorang untuk melakukan jenayah, sama ada terhadap seseorang, organisasi, kerajaan, negara atau harta-benda orang lain. Kesalahan-kesalahan ini termasuklah perlakuan serangan yang dilakukan ke atas sistem komputer, sistem rangkaian komputer semata-mata untuk memperolehi maklumat yang bermanfaat tersimpan didalam sistem komputer. Di samping turut melakukan jenayah 'tradisi' yang lain seperti merancang kegiatan keganasan (terrorism), pengedaran 'bahan-bahan terlarang' (i.e. dadah, pornografi), penipuan dan lain-lainnya dengan menggunakan komputer. Kertas ini cuba untuk mengemukakan jenis-jenis, permasalahan dan tindakan kawalan terhadap e-jenayah.

ABSTRACT

The Internet is the greatest technological innovation since the achievement of the industrial revolution, accomplished through amalgamation of information, communication and digital technology which then created the largest and widest ever computer networking system. Therefore, new sphere known as the Internet which is virtual in nature, also prominently name as cyber-world. Consequently, whole new structures of political, economy, social and culturally of society have been forced into us to accept the changes which then inaugurate with new electronic practices. Eventually, the Internet was created by the use of inter networking of the computing system throughout the world with help of automated data system. Subsequently, open-up the new frontier of digital development. Unfortunately, this new infrastructure also open-up gap for new breed of criminals to adopt this technologically driven by 'digitizing' the traditional crimes with the new opportunities. With all computing tools and electronic gadgets which they could hold, its seem easier for them to launch attack in the direction of individual, organizations, groups and even governments in no time. Their capabilities not only be able to commit 'traditional' crimes with sophisticated ways, its also pave new electronic crimes which even harder for enforcement to bring them down. This paper will explain types of electronic crime, problems created and methods to control e-criminals.

PENGHARGAAN

Dengan Nama ALLAH Yang Maha Pemurah dan Maha Pengasih – Bersyukur ke hadrat Illahi kerana dengan izinNya usaha ini telah dapat disempurnakan. Saya ingin menyampaikan ucapan penghargaan kepada Prof. Dr. Ab. Hadi Zakaria, atas bimbingan dan tunjuk ajar yang telah diberikan. Terima kasih tidak terhingga diberikan kepada Prof. Dr. Rahimah A. Aziz yang memberi penuh kepercayaan untuk mengendalikan operasi penyelidikannya dan memberi sokongan sepanjang saya menjalani program ini dan Prof. Madya Dr. Kamaruddin M. Said yang telah banyak memberi perangsang dan semangat kepada saya. Tidak dilupakan juga kepada semua anggota Jabatan Antropologi & Sosiologi, FSSK, UKM Bangi yang turut membantu secara langsung dan tidak langsung serta sokongan padu mereka. Untuk QRT (Ju, Ma, Nasrul dan Su) yang sentiasa tangkas, cekal dan boleh diharapkan telah banyak membantu saya dalam menjalankan tugas dan tanggungjawab sewaktu mengendalikan kerja di lapangan. Untuk MCJs 2001/2, pengalaman bersama banyak memberi semangat untuk terus berusaha! Untuk semua teruskan "Perjuangan yg belum Selesai". Tidak ketinggalan isteri dan anak-anak tersayang yang sentiasa faham dengan beban dan tugas Babah, pengorbanan semua amat dihargai dan disanjung tinggi.

KANDUNGAN

BAB 1

1. Pengenalan

Terjahan kemajuan teknologi komputer dan diikuti dengan Internet semenjak 15 tahun yang lampau telah meletakkannya sebagai satu kuasa perubahan yang amat besar ke atas berbagai perspektif kehidupan masyarakat yang merangkumi dari segi sejarah, kerajaan, hinggalah kepada dunia korporat mahupun individu di alaf baru ini. Rangkuman perubahan yang amat pesat dan luas ini memperlihatkan bagaimana keupayaan komputer dan teknologi digital mampu menyediakan berbagai bentuk kemudahan, seperti penyimpanan data elektronik, pemindahan maklumat, pemerosesan dan penggunaan data, hingga kepada memanipulasi segala maklumat binari oleh mereka yang tidak bertanggung jawab (Denning & Denning, 1997). Maka tidak hairanlah wujud satu lanskap baru dalam dunia kehidupan era digital ini yang juga dikenali sebagai ruang siber – *cyberspace* – yang serba canggih, moden dan lahir dalam "sekelip mata". Penjelmaan ruang siber telah banyak digambarkan terutama sekali melalui filem cereka yang dihasilkan oleh Hollywood, sejak dari filem *"Neuromencer"* ke filem lakonan Sandra Bullock *"The Net"*, manakala kemampuan teknologi diperlihatkan juga dalam filem *"Enemy of the State"*. Dari gambaran yang diperlihatkan, ruang siber memiliki serba kelebihan dan keistimewaan untuk diisi dengan segala macam kemungkinan dan peluang.

Di Malaysia pertumbuhan teknologi maklumat dan komunikasi (ICT) telah mempercepatkan lagi arus perubahan terutama sekali ke arah membentuk sebuah masyarakat Malaysia yang bersifat global. Kesediaan merebut peluang yang dijanjikan oleh teknologi maklumat, komunikasi dan multimedia membolehkan masyarakat bermaklumat terbentuk seperti yang sering diwarwarkan oleh kerajaan. Malahan **Wawasan 2020** Malaysia telah menetapkan salah satu prinsip dasarnya adalah untuk membentuk masyarakat berpengetahuan (*knowledge society).* Hal ini sekali gus memberi harapan agar masyarakat negara ini tidak hanya tahu menerima dan menggunakan teknologi, tetapi turut terbabit dalam inovasi dan penciptaan (invention) teknologi baru yang bakal menyumbang kepada peradaban sains dan teknologi di masa akan datang. Dengan kata lain negara akan dapat melahirkan lebih ramai tenaga kerja berpengetahuan (*knowledge workers*) tinggi.

Dalam era digital kini teknologi ICT bukan saja digunakan secara meluas untuk memenuhi pelbagai fungsi di sektor industri dan ekonomi, tetapi juga turut berperanan sebagai alat pengantungan hidup (Ford et. al., 1997). Kepenggunaan dan kepegantungan (dependency) teknologi, khususnya dalam bidang perubatan dan pengangkutan (misalnya penerbangan) membuktikan hal ini. Dengan ini boleh diandaikan bahawa sekiranya 'alat' ini gagal berfungsi dengan sempurna boleh mengakibatnya nyawa manusia terancam. Keadaan ini meletakkan kehidupan manusia seolah-olah perlu tunduk dan akur dengan

kejituan dan ketepatan peralatan yang berkaitan, yang menjadi nadi (DNS-Digital Nervous System) kepada segala urusan seharian masakini. Bahkan, kecenderungan ini mewujudkan kadar kepegantungan yang tinggi kepada teknologi ICT dan secara langsung atau tidak langsung 'memaksa' kita menerima nilai kehidupan berkomputer.

Keadaan sedemikian meletakkan keseluruhan anggota masyarakat hari ini kepada pelbagai risiko bersifat positif dan negatif dalam kehidupan seharian mereka. Hal ini ditunjukkan melalui tindakan masyarakat dunia mengambil berbagai langkah persediaan selain memperuntukkan ribuan billion ringgit semata-mata kerana takut kepada kemungkinan buruk yang 'kononnya' akan berpunca dari pepijat alaf (millennium bug) dan menjejaskan atau melumpuhkan keseluruhan pengendalian operasi komputer dan peralatan yang berkaitan dengan komputer. Ancaman ini dikatakan akan berlaku sebaik sahaja tahun 2000 bermula kerana sesetengah cip di dalam perkakasan komputer akan menjadi kacau-bilau semata-mata kerana komputer atau sistem berkenaan tidak mampu untuk mengenali angka 2000 dan dengan itu, akan kembali ke angka 1900.

'Malangnya', masalah yang dijangkakan itu didapati tidak meninggalkan kesan besar. Walau bagaimanapun, peristiwa ini sudah cukup untuk menunjukkan tahap pengantungan yang tinggi masyarakat dunia hari ini kepada komputer dan prasarana digital yang sedia ada. Situasi berkenaan juga

menunjukkan setakat mana sistem komputer tidak hanya menyediakan kemudahan, tetapi mampu mengakibatkan kemusnahan atau *'holocust'*.

Oleh itu tanpa sebarang kawalan atau tindakan mencegah (preventive measures) masyarakat hari ini akan lebih terdedah sama ada secara langsung atau tidak langsung kepada ancaman dari pelaku e-jenayah atau disebut juga *"cyber-criminals"* (Sterling, 1993). Sebarang perlakuan seperti memasuki sistem rangkaian komputer akan mengakibatkan kesan kemusnahan yang sudah tentu akan membawa kepada pelbagai permasalahan yang lain. Lebih-lebih lagi dengan wujudnya 'dunia tanpa sempadan', negara kini terdedah kepada berbagai entiti yang bergerak melewati batas persempadanan geografikal dan politik sesuatu negara (Strassman, 1995). Lantas kemungkinan untuk anggota masyarakat hari ini menjadi mangsa e-jenayah amat tinggi risikonya selari dengan tahap penggantungannya kepada teknologi digital itu. Pendekatan 'tradisional' melindungi dan mengawasi wilayah penguasaan negara seperti sebelumnya sudah tidak mencukupi, justeru adalah perlu memahami maksud sebenar ciri-ciri dan sifat alam siber supaya ancaman yang seumpama akan dapat dibendung dan ditangani.

Tambahan pula dikatakan pelaku e-jenayah mampu untuk melakukan berbagai tindakan seperti memanipulasi sistem komputer sama ada untuk kepentingan diri ataupun kepentingan orang lain dari mana-mana tempat di dunia ini (Hafner & Markoff, 1995). Peluang untuk memanipulasikan

prasarana ICT masa kini sentiasa wujud memandangkan sistem komputer hari ini dihubungkan pula dengan satu jaringan rangkaian komputer yang luas yang dikenali sebagai Internet. Teknologi ini bukan sahaja mampu membawa jutaan maklumat dalam sekelip mata, malah dengan sekelip mata juga (seandainya pelaku e-jenayah, bertindak) pelaku e-jenayah mampu untuk melumpuhkan sistem komputer milik seseorang, atau korporat mahupun kerajaan hingga boleh menjejaskan negara sama ada dari segi politik, ekonomi atau sosial (Garfinkel & Spafford, 1997).

Akibat keresahan dan kegusaran berkaitan ancaman ini sering disuarakan oleh ramai pihak tentang perlunya perkara tersebut diberi perhatian yang serius dan ditangani dengan cara yang terbaik, dan seharusnya bersifat progresif lagi berkesan. Jika tidak pelaku e-jenayah ini akan menyebabkan hak kawalan ke atas legitimasi ICT akan terlepas. Kawalan bukan sahaja merupakan asas dan teras kedaulatan sesebuah negara, tetapi menentukan daya mampu pemerintah menguruskan hal-ehwal. Maka, ancaman sedemikian mungkin boleh menyebabkan keupayaan berkenaan terjejas sama sekali.

Kertas ini akan cuba menyelami berbagai-bagai perubahan yang sedang berlaku ke atas kehidupan masyarakat di era digital secara umum. Secara khusus akan memperincikan perbincangan kepada jenis-jenis e-jenayah yang berlaku dalam era digital ini, ancaman yang mungkin ditinggalkan dan langkah-

langkah yang telah, sedang dan boleh dilakukan termasuk langkah kawalan dari segi undang-undang.

Metodologi Penyelidikan

Kajian mengenai e-jenayah ini dilakukan dengan mengambil pendekatan kajian kepustakaan (library research). Berdasarkan kepada kaedah ini, berbagai maklumat yang sedia terhimpun dapat digunakan bagi menjelaskan tentang e-jenayah yang menjadi ancaman di alaf yang baru ini. Ditambah pula kefahaman tentang e-jenayah perlu diterangkan dengan lebih menyeluruh supaya rupa bentuk e-jenayah dapat diperjelaskan secara sebaik mungkin. Di samping itu perhatian turut diberikan kepada karya-karya khusus yang berkeupayaan untuk menjelaskan tentang e-jenayah secara menyeluruh. Di samping akan menggunakan sumber rujukan dari laman-laman web yang berkaitan khususnya yang tertumpu kepada isu sekuriti komputer dan Internet.

Oleh itu pendekatan ini amat sesuai dengan kerperluan penyelidikan yang dilakukan bagi melengkapkan kertas projek ini. Secara sistematiknya penghuraian dikemukakan dengan dimulakan tentang komputer dan Internet. Tujuannya bagi memberi penjelasan umum mengenai perkara berkenaan dan diikuti dengan huraian yang menyeluruh untuk menerangkan hubungan antara komputer dan Internet dengan kegiatan e-jenayah. Pada masa yang sama contoh-contoh yang sesuai dan berkaitan turut dikemukakan bagi membolehkan penjelasan dibuat mengenai keupayaan dan ancaman e-jenayah

pada masa kini. Dengan memberi tumpuan yang seumpama ini, pemahaman tentang aktiviti e-jenayah dapat dihuraikan secara serentak dengan penjelasan tentang penggunaan komputer dan Internet.

Sungguhpun begitu adalah tidak mungkin untuk membongkarkan secara terperinci mengenai bentuk-bentuk ancaman e-jenayah yang berlaku secara komprehensif dewasa ini. Ini adalah kerana jika kajian yang lebih terperinci ingin dilakukan maka amat wajar diadakan penyelidikan secara kajian kes. Walau bagaimanapun, memandangkan isu yang diperbincangkan adalah amat luas dan memerlukan penyelidikan yang menyeluruh dan rapi, penulis terpaksa menghadkan penyelidikan ini dengan hanya berlandaskan sumber maklumat sekunder sahaja. Untuk itu penulis lebih memusatkan perbincangan kepada kewujudan ancaman e-jenayah yang semakin berleluasa dan bagaimana ancaman ini akan memberi kesan ke atas kehidupan masyarakat di alaf ini. Kedua-dua pokok perbincangan yang menjadi tunjang kepada kepada penyelidikan ini dan dijadikan sebagai tunggak pembicaraan bagi keseluruhan kertas projek ini.

BAB 2

2. Komputer & Internet

Pada pengertian umum komputer didefinisikan sebagai alat yang mampu melaksanakan peranan sebagai penerima input, memproses (mengikut ketetapan) dan menghasilkan keputusan yang diinginkan[1]. Manakala Internet[2] pula adalah satu jaringan komputer yang dihubungkan antara satu sama lain. Hasil dari gabungan komputer dan Internet, corak kehidupan masyarakat hari ini telah banyak mengubah cara berkomunikasi, berjual-beli barang dan juga memperolehi perkhidmatan. Ternyata teknologi komputer dan Internet yang berteraskan kepada ICT pada masa kini terbukti berkemampuan bukan hanya untuk membantu menjayakan ekonomi negara misalnya dalam bidang perniagaan, perindustrian, mempertingkatkan tahap komunikasi yang efisyen, dan juga mampu untuk menjadikan tenaga pekerja lebih produktif.

Hari ini, adalah dianggarkan bahawa pengguna Internet diseluruh dunia seramai 400 juta orang, di Malaysia sahaja terdapat 3 240 000 orang pengguna (Februari 2002) di Amerika Syarikat pula dianggarkan seramai 108 500 000 orang pengguna (Januari 2002) berdasarkan kepada survei yang dikendalikan

---

[1] *Microsoft Computer Dictionary Fifth Edition, 2001.*Microsoft Press

[2] *Internet* didefinisikan sebagai *"collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio."*

oleh Ipsos-Reid[3]. Jumlah ini sentiasa meningkat dari hari ke hari dan dijangkakan pengguna Internet yang akan melanggani perkhidmatan ini pada 2005 akan meningkat keangka 1 billion[4]. (Dr. Angus Reid – Chairman dan CEO Angus Reid Group).

Sememangnya telah sedia maklum keupayaan positif yang ditunjukkan oleh penggunaan teknologi komputer pada masa kini, tetapi tidak dapat dinafikan komputer juga mampu dimanipulasi, dan dijadikan sebagai alat untuk melaksanakan berbagai perlakuan menyalahi undang-undang. Dengan kata lain, gabungan Internet dan komputer boleh bertindak sebagai *medium* yang amat sesuai kepada mana-mana pihak untuk membolehkan mereka merancang dan menyempurnakan berbagai tindakan yang bercanggah dengan undang-undang yang ada pada hari ini[5]. Seringkali didapati tindakan yang dilakukan oleh golongan ini adalah untuk memanipulasikan teknologi maklumat bagi kepentingan diri.

Ini bermakna segala bentuk maklumat yang sedia tersimpan sama ada maklumat umum mahupun maklumat sensitif dan berharga (dari segi nilainya) atau pun maklumat peribadi di dalam sistem pengstoran komputer. Segala maklumat ini sentiasa tersedia untuk diakses untuk keperluan sesuatu tugas pada bila-bila masa. Pada masa yang sama kemungkinan terdapat pula pihak-

[3] Seperti mana yang dilaporkan oleh Ipsos-Reid dilaman web http://www.angusreid.com/latest.cfm
[4] Ipsos-Reid dilaman web http://www.angusreid.com
[5] National Institute of Justice (2000) *Crime Scene Investigation: A Guide for Law Enforcement.* Washington D.C., Department of Justice, National Institute of Justice., NCJ 178280.

pihak tertentu (yang memiliki niat lain), misalnya ingin memperolehi maklumat berkenaan bagi tujuan negatif. Sebagai contohnya seorang 'penggodam' (hackers) yang bertindak mengakses sistem komputer sama ada atas kepentingan peribadi atau diupah oleh pihak tertentu untuk memperolehi sesuatu maklumat (McClure et. al., 1999). Akibatnya tindakan golongan ini sudah tentu akan menggugat intergriti sesuatu sistem maklumat, terutama sekali apabila mereka berjaya memperolehi maklumat yang diinginkan. Malahan akan menjadi lebih teruk lagi apabila mereka bertindak meminda atau memusnahkan maklumat yang terdapat di pengkalan data yang telah mereka akses.

Didapati situasi seumpama kini menjadi semakin galak dan kadangkala sukar dikesan apatah lagi untuk mendakwa atau mengambil tindakan undang-undang ke atas golongan berkenaan.

Pada umumnya seperti kebanyakan teknologi baru (seperti Internet) yang diperkenalkan seharusnya memiliki keupayaan yang bertujuan untuk memberi kemudahan dan kesenangan kepada kehidupan sosial manusia. Namun pada masa yang sama tidak dapat dinafikan kesan negatif tetap tidak dapat dielakkan. Ini kerana kehadiran teknologi baru seperti ini tetap akan mengundang gejala buruk. Misalnya selepas kehadiran telefon, gejala negatif seperti *phone-phreaking* yang bertujuan untuk menyalahgunakan kemudahan perkhidmatan panggilan seperti *toll-free* untuk membolehkan panggilan jauh

dilakukan dengan percuma (McClure et. al., 1999). Begitu juga dengan tindakan menggunakan telefon untuk tujuan *harrasment* terhadap pihak-pihak tertentu.

Ini bermakna kemudahan Internet turut digunakan secara meluas untuk berbagai tindakan yang bertujuan negatif. Antara tahun 1999 hingga tahun 2000 telah berlaku tindakan mengedar virus atau cecacing (worm) secara meluas di seluruh dunia melalui sistem edaran e-mel antaranya *"Melisa"*, *"Code Red Worm"*, *"Nimda.Sir"* dan *"Explore.Zip.Worm"* hingga menyebabkan berlakunya kerosakan yang besar ke sistem komputer dan rangkaian komputer milik peribadi atau organisasi seperti memadam fail yang terkandung di dalamnya dan juga menyebabkan sistem komputer menjadi lumpuh (Ludwig, 1998). Akibatnya kerugian jutaan ringgit terpaksa ditanggung oleh individu mahupun organisasi. Selain dari itu, tindakan menjejaskan laman web milik pengguna persendirian dan laman-web pedagangan (e-commerce) yang lumpuh turut berlaku akibat dari tindakan seperti *"denial of service"*[6] dan ada pula laman-laman web yang dicacatkan melalui kaedah *"page-jacking"*

[6] Sila rujuk Lampiran II, ms viii.

2.1 Internet: memahami operasinya

Sehingga kini semakin ramai yang mungkin pernah mendengar tentang Internet dan jumlah pengguna Internet di seluruh dunia semakin meningkat setiap hari. Namun kadar penggunaan Internet di Malaysia dianggap rendah berbanding dengan negara-negara maju yang lain. Bahkan kurang dari 15% yang menggunakan dan mempunyai kemudahan Internet[7]. Internet merupakan berpuluh-puluh rangkaian sistem yang dihubungkan di seluruh dunia. Dari segi istilahnya iaitu "INTERNETworks", sudahpun menerangkan keadaan itu yang memberi pengertian lebih dari satu rangkaian komputer yang berkomunikasi antaranya. Komputer ini berkomunikasi dalam satu sistem rangkaian dan saling berhubungan dengan sistem rangkaian komputer yang lain dengan menggunakan protokol komunikasi yang ditetapkan. Dari segi operasinya, seolah-olah rangkaian Internet terdiri dari satu gabungan rangkaian sistem komputer gergasi, yang saling berkomunikasi dan bertukar maklumat (data).

Selain dari Internet, terdapat juga *Intranets* iaitu sistem rangkaian komputer (lebih 'luas' dari *Local Area Network* atau *Wide Area Network*) yang saling berhubungan dalam satu organisasi dan menggunakan teknologi komunikasi Internet, walaupun secara fizikalnya tidak berada dalam lingkungan

[7] Ipsos-Reid di laman web http://www.angusreid.com

fizikal yang sama. Manakala *Extranets* merujuk kepada kegunaan hubungan antara sistem rangkaian komputer yang dimiliki oleh lebih dari satu organisasi tetapi saling berhubung atas sebab kepentingan hubungan dagangan misalnya. Ketiga-tiga jenis teknologi komunikasi yang disebut di atas merupakan tulang belakang fizikal keseluruhan pengoperasian Internet.

Perlu juga difahami bahawa Internet adalah merupakan satu bentuk kemudahan teknologi komunikasi yang memiliki keupayaan untuk menghantar data atau maklumat dalam berbagai bentuk. Perkhidmatan dan kemudahan Internet kini semakin popular dan sering digunakan kerana berkeupayaan untuk menghantar maklumat dalam bentuk *multimedia* (seperti teks, audio, video dan grafik) yang disempurnakan sama ada melalui;

i. *World Wide Web* (WWW)

ii. *Electronic Mail* (e-mel)

iii. *Newsgroups & Mailing List*

iv. *Chat*

Dari segi penggunaannya, sesiapa sahaja yang mempunyai kemudahan mengakses Internet boleh menggunakannya untuk berbagai jenis tujuan, termasuk juga bagi tujuan e-jenayah. Dari segi teori, oleh kerana sistem komputer ini saling berhubungan antara sistem rangkaian komputer, maka jenis kegiatan ini boleh dikesan secara digital. Sungguhpun begitu, terdapat

juga antaranya yang tidak dapat dikesan kerana mereka yang menggunakannya dengan sengaja cuba untuk mengelakkan diri mereka dari dikesan. Lebih-lebih lagi apabila seseorang pengguna itu dengan sengaja mengambil beberapa langkah khusus untuk menghilangkan jejak digitalnya supaya tidak ada orang yang tahu mengenai aktivitinya.

World Wide Web (WWW) – bolehlah dianggap sebagai satu perpustakaan yang terkandung di dalamnya dokumen dalam berbagai format *multimedia.* Ia juga selalu disebut sebagai Laman Web – *web pages* – dan boleh diakses dari mana-mana sahaja asalkan terdapat kemudahan Internet. Jika hendak dianalogikan dapatlah dikatakan ia sebagai satu perpustakaan teramat besar. Dengan hanya menggunakan pelayar – *browser* – seseorang pengguna sudah berupaya mengakses berbilion muka surat dokumen, sama ada dalam bentuk teks, audio, *visual* dan lain-lain lagi. Semua maklumat ini tersusun mengikut agihan laman-web masing-masing dan boleh diperolehi dengan menggunakan enjin gelintar – *search engine*[8] – misalnya dengan hanya memasukkan istilah carian pada laman web yang khusus bagi membuat carian satu senarai rujuk silang (cross-reference) dengan hiperpautan (hyperlink) bagi tujuan menghubungkan carian ke laman web yang diperlukan.

Dari situ pengguna boleh menggunakan pautan – *link* – yang biasanya disenaraikan di laman-laman web berkenaan. Kaedah ini membolehkan

[8] Antara enjin gelintar yang popular ialah www.yahoo.com, www.ask.com dan www.google.com.

seseorang itu terus melayari Internet dari satu alamat ke satu alamat yang lain bagi memperolehi maklumat yang diperlukan. Seperkara yang lain, hampir semua laman web boleh diakses tanpa sebarang sekatan atau halangan. Seseorang tidak perlu memperolehi kebenaran untuk melayari sesuatu laman web, malahan pemilik juga 'tidak akan mengetahui' siapa yang melayari laman webnya (kecuali diwujudkan *sniffer*[9] untuk mengesan dengan memasukkan *'dynamic cookies'*). Manakala kandungan laman web pula mungkin tersimpan di pelayan web dan boleh diletakkan di mana-mana sahaja, asalkan terdapatnya hubungan talian Internet.

Electronic Mail (e-mel) – selain dari laman web, e-mel adalah kaedah komunikasi yang sangat popular di era Internet. Fungsinya seperti menghantar surat secara konvensional. E-mel membolehkan seseorang itu menghantar mesej dan boleh juga disertakan fail dalam format *multimedia* kepada sesiapa sahaja yang mempunyai alamat e-mel dan kepada pemilik telefon mudahalih dan ke komputer telapak melalui sistem pesanan ringkas (sms) atau sistem pesanan multimedia (mms). Walau bagaimanapun dari segi pengoperasiannya agak kompleks kerana ia melibatkan penggunaan perisian khusus, dengan protokol penghantaran tertentu, dan juga perlunya pelayan e-mel bagi membolehkan keseluruhan proses disempurnakan. Namun begitu, dari segi

[9] Sejenis program yang ditugaskan secara khusus untuk merekodkan maklumat/data dari pengguna yang melawati sesuatu laman web.

penggunaan amat mudah dan ringkas, ditambah pula kemampuan penghantaran e-mel yang cekap dan cepat.

Pada satu-satu masa terdapat jutaan e-mel yang berlegar dalam laluan Internet di seluruh dunia, yang kadangkala dipisahkan bagi tujuan pemindahan tetapi dicantumkan semula dipengakhirannya sebelum sampai kepada penerima. Kemudahan ini sangat mudah disalah gunakan oleh berbagai pihak terutama yang ingin melakukan e-jenayah. Bahkan ia paling mudah digunakan sewaktu perancangan dijalankan sehingga sebelum kegiatan dijalankan. Sebagaimana yang telah dinyatakan, e-mel yang dihantar boleh disertakan juga dokumen *multimedia* seperti bahan grafik termasuk yang bersifat interaktif dan animasi. Sehubungan itu, maka sudah tentulah pengamal pedofil misalnya dapat menggunakan kemudahan ini bagi mengedar grafik lucah dan sebagainya.

Newsgroups & Mailing List – kemudahan ini adalah merupakan platform diskusi antara pengguna yang boleh dilakukan secara dua hala, apabila seseorang itu menghantar mesej ke *newsgroups* sesiapa saja yang 'berlanggan' akan dapat membalas balik mesej atau memberi komen kepada artikel yang berkenaan. Pembahagian *newsgroups* selalunya mengikut kategori negara, bahasa dan minat serta kecenderungan kepada sesuatu aspek. Terdapat puluhan ribu *newsgroups* yang boleh dilanggan oleh pengguna Internet, walau bagaimanapun tidak semua *newsgroups* boleh diperolehi dari pelayan berita (news-server).

Namun begitu, jika seseorang pengguna Internet lokal tidak dapat mengakses *newsgroups* melalui ISP lokalnya, mereka boleh mengaksesnya melalui kaedah khusus dari sumber lain. Keistimewaan utama *newsgroups* ialah pengguna yang berlanggan tidak perlu memberikan sebarang butiran peribadi mereka. Malahan masing-masing boleh terus kekal berkomunikasi tanpa perlu memperkenalkan diri kecuali nama samaran (*handle*) yang digunakan di laman *chat* yang berkenaan.

Chat - satu lagi kemudahan 'istimewa' kerana pengguna boleh berkomunikasi secara *real-time* dengan pengguna yang lain. Kemudahan ini juga kini telah dipertingkatkan lagi dengan penggunaan kamera web yang membolehkan *video-text-voice over Internet* dilaksanakan. Sistem chat yang terbesar sekali dan paling popular ialah *Internet Relay Chat – IRC –* yang membolehkan seseorang itu berhubungan dengan sesiapa sahaja dan di mana-mana sahaja lokasinya di dunia ini. Kemudahan ini dianggap sebagai salah satu kemudahan yang terawal dalam era Internet dan masih lagi popular di kalangan remaja khususnya. Kemudahan ini juga mungkin turut digunakan oleh pelaku e-jenayah yang didapati cuba menggerakkan kegiatannya diperingkat global seperti golongan *cyberterrorist.* Selain dari itu disebabkan oleh pengguna tidak perlu memperkenalkan diri mereka lebih dari yang diperlukan, maka mereka sentiasa boleh menggunakan nama samaran.

2.1.1 Alamat Internet

Keseluruhan operasi Internet melibatkan satu sistem hubungan atau komunikasi yang kompleks dengan menggunakan alamat khusus bagi mengenal-pasti sesuatu alamat laman web dan mesej e-mel yang dihantar. Sesuatu laman web memiliki laman domain yang khusus dan didaftarkan supaya tidak berlaku kecelaruan dalam memperolehi maklumat yang diperlukan. Manakala alamat e-mel pula adalah berdasarkan domain yang didaftarkan. Di samping itu alamat laman domain itu pula dikategorikan mengikut sifat (walaupun perkara ini bukan satu kemestian). Sebagai contoh Universiti Malaya menggunakan domain *'edu'* bagi memperlihatkan sifatnya sebagai pusat pengajian tinggi.

Kesemua alamat domain ini dirujuk pula kepada *"IP Address"* yang selalunya dapat dikenal pasti seperti berikut 202.185.55.22. Hampir setiap komputer yang ingin dihubungkan ke platform Internet mesti memiliki alamat IP yang seumpamanya. Tanpa alamat berkenaan komputer berkenaan tidak akan dapat mengakses ke Internet atau berkomunikasi dengan komputer yang lain. Alamat yang digunakan biasanya statik tetapi terdapat juga kaedah menggunakan alamat IP yang dinamik, terutama sekali pelanggan Internet individu yang menggunakan perkhidmatan *dial-up access*. Walau bagaimanapun, pengguna hanya perlu menggunakan alamat domain dan tidak menggunakan

alamat IP untuk melayari laman web dan bagi memudahkan pengenalan dan carian sesuatu laman web.

Oleh itu didapati alamat seperti http://www.um.edu.my adalah alamat domain utama, sementara dokumen atau fail atau maklumat lain ditempatkan di sub-domain seperti http://www.um.edu.my/FU2/Index.htm yang merujuk kepada Fakulti Undang-undang. Kesemua alamat laman web adalah unik dan boleh dikesan dengan menggunakan URL – *Universal Resourse Locator* – manakala alamat domain pula menggunakan http (*Hyper Text Mark-up Language*) sebagai penghubung antara mereka yang bersifat sejagat.

2.1.2 Pengguna Internet

Boleh dikatakan sesiapa sahaja boleh dianggap sebagai pengguna Internet asalkan mereka boleh mengakses ke Internet, dan pada masa yang sama sebahagian besar dari pengguna juga boleh bertindak sebagai 'pemberi' maklumat di Internet. Pada umumnya maklumat yang ditawarkan ada terdapat di laman-laman web yang terdapat hari ini. Ianya disediakan oleh kerajaan, organisasi seperti syarikat atau pertubuhan dan juga individu.

Kepesatan perkembangan teknologi ICT pada hari ini telah menyebabkan Internet menjadi medium hubungan yang terpenting. Selain itu adalah mudah untuk menerbitkan sesuatu laman web dan dapat dijayakan dalam jangkamasa yang singkat. Secara umum terdapat tiga golongan yang

mudah dikenal pasti iaitu pengguna (terdiri dari individu, organisasi, syarikat dan kerajaan) Internet. Golongan kedua dikenali sebagai penyalur maklumat – *content providers* – yang terdiri dari berbagai golongan sama ada di peringkat lokal atau antarabangsa. Manakala golongan yang ketiga adalah dari kalangan pembekal khidmat Internet (ISP), yang bertanggung jawab menyediakan rangkaian hubungan sistem komputer individu atau satu sistem rangkaian ke platform Internet. Antara bentuk atau kaedah penyambungan yang ditawarkan ialah kaedah *dail-up* yang menggunakan talian tetap (telefon) atau *Intergrated Switch Digital Network* atau hubungan terus dengan kemudahan Internet jalurlebar (broadband).

Kepesatan kemajuan teknologi ICT yang pada hari ini turut menyediakan kaedah mendapatkan hubungan ke Internet tanpa wayar. Misalnya dalam perkhidmatan telefon mudahalih (tahap *2G*) kaedah *Wireless Application Protocol – WAP-* digunakan. Manakala bagi peringkat teknologi tahap *2.5G* yang menggunakan sistem hubungan *GPRS* (General Packet Radio Signal), kemampuannya bukan setakat menghantar maklumat dalam bentuk teks (seperti sms) tetapi juga dalam format grafik dengan menggunakan kaedah sistem pesanan multimedia (mms)

Dengan berbagai kemudahan yang disediakan dan kehadiran teknologi yang lebih canggih, pengguna Internet pada masa kini dan akan datang dapat menikmati kemudahan yang lebih baik. Bukan sahaja adanya kaedah

hubungan yang lebih berkesan tetapi juga boleh mencapai maklumat yang lebih ekstensif dan berguna. Pada masa yang sama pengguna daripada kalangan pelajar sekolah dan institusi pengajian tinggi terutamanya akan dapat menggunakan Internet sebagai sumber rujukan dan penyelidikan terutama bagi mendapatkan maklumat yang terkini.

BAB 3

3. Komputer & Internet: Keupayaan dan Ancaman

Kemudahan dan kecekapan ICT hari ini menjadikan kegiatan komunikasi, memperolehi maklumat, dan menyebarkan propaganda sangat praktikal, cepat dan murah lebih-lebih lagi ianya bersifat global. Dengan kata lain, *technological empowerment* memberi berbagai faedah positif dan negatif kepada setiap individu, organisasi dan negara untuk melaksanakan berbagai kegiatan. Namun begitu, kehadiran sesetengah golongan yang cuba menggunakan Internet sebagai platform untuk mereka melancarkan berbagai kegiatan dan tindakan luar undang-undang sudah tentu akan memberi berbagai kesan negatif hingga memerlukan pihak penguatkuasa (authority) dan kerajaan (state) memberi perhatian terutama sekali dari segi melaksanakan polisi termasuk undang-undang untuk menghadapi golongan yang dikategorikan sebagai pelaku e-jenayah. Berikut adalah beberapa perlakuan yang berasaskan keupayaan dan kemampuan teknologi Internet (Wall, 2000).

3.1 Realiti Keupayaan e-jenayah

Pengumpulan – Internet diumpamakan sebuah perpustakaan yang terbesar di dunia yang memiliki berbagai jenis maklumat. Jumlah bilangan

laman web telah pun melebihi angka billion dari segi halamannya dan kebanyakannya boleh diperolehi dengan 'percuma' secara terus dari komputer peribadi, komputer bimbit, komputer telapak malahan juga telefon mudah-alih asalkan mempunyai akses internet. Oleh itu adalah mudah buat masa kini untuk seseorang itu mendapatkan apa saja maklumat, misalnya maklumat dari pihak kerajaan seperti dokumen legislatif, pengumuman atau warta kerajaan, perbincangan mengenai isu semasa, pandangan umum yang berkaitan dengan isu-isu berkaitan.

Kelebihan utama ruang siber ialah kerana tiada sebarang halangan bersifat *'censorship'*[10] dan jika ada pun tidak dapat dikuatkuasakan sepenuhnya[11] atau diwujudkan. Sebagai contoh apabila kerajaan Jordan bertindak mengenakan sekatan jualan ke atas satu terbitan majalah antarabangsa (The Economist), pembaca kemudiannya telah beralih ke ruang siber dan memperolehinya secara 'atas-talian' (online) dan kemudiannya difotokopi untuk edaran. Adalah dipercayai edaran dalam bentuk fotokopi menjangkau 1,000 naskah[12] dan kemudian difaks di kalangan aktivis atau mereka yang berminat. Ini jelas membuktikan kelompok yang memiliki kecenderungan untuk memperolehi maklumat yang diperlukan akan beralih ke ruang siber.

---

[10] Salah satu matlamat perjuangan kelompok-kelompok ini adalah hak bersuara, menwujudkan sebarang bentuk kawalan atau tapisan disifatkan sebagai menyekat hak asasi manusia

[11] Walaupun sesetengah negara seperti China mengenakan sekatan ke atas trafik maklumat Internet

[12] Alan Doherty, *A Net: Journalist Outwit Censors*, Wired News, March 13, 1999

Sungguhpun begitu terdapat juga sesetengah negara yang mengambil langkah untuk mengawal trafik-maklumat Internet. Langkah ini dilakukan bagi mengawal agar unsur-unsur pengaruh luar tidak 'meracuni' pemikiran rakyatnya memandangkan maklumat yang tersebar di ruang siber sentiasa boleh diperolehi dengan murah, mudah, cekap dan cepat. Sungguhpun begitu, kebanyakan negara sedar dan akui tentang kelebihan ruang siber untuk membantu ke arah mempertingkatkan tahap dan langkahan kemajuan. Walau bagaimanapun rasa curiga tetap wujud kerana terdapatnya kemungkinan kesan negatif akan meninggalkan impak signifikan ke atas politik lokal (Rosenoer, 1997). Di Malaysia, sungguhpun kerajaan berkali-kali menggesa rakyat supaya berwaspada dengan maklumat (politik khususnya) yang diperolehi dari Internet, tetapi tiada sebarang usaha dilakukan untuk menapis trafik-maklumat berkenaan.

Di negara China, langkah sekatan yang dianggap ekstrim yang telah dilakukan bukan sahaja menghalang pengguna Internet melayari laman-laman web tertentu[13], tetapi juga turut menjalankan saringan ke atas e-mel pengguna Internet tempatan. Ini terbukti apabila Lin Hai bertindak menjual 30 ribu alamat e-mel kepada kumpulan pergerakan pro-demokrasi yang beroperasi di

[13] Pengguna Internet di China tidak diizinkan mengakses laman cnn.com

Washington. Beliau telah dikenakan hukuman 2 tahun penjara dan denda 10,000 Yuan[14].

Dalam keadaan yang agak berbeza, di Yugoslavia sewaktu konflik Kosovo memuncak, Internet menjadi platform utama untuk menerima dan menyampaikan maklumat semasa. Dalam kes di sana, penduduk tempatan menyifatkan NATO dan Amerika Syarikat sengaja menggembar-gemburkan keganasan tentera Serb di negara-negara Balkan yang berkonflik dengan Yugoslavia. Sehingga timbul wacana anti-NATO dan Amerika Syarikat di Belgrade melalui ruang siber di negara berkenaan.

Penerbitan – menerbitkan melalui ruang siber adalah kaedah paling cepat, mudah dan murah, termasuk dapat mempastikan sama ada bahan terbitan diedarkan secara meluas (Deffie & Landau, 1998). Sebaliknya begitu cepat, mudah dan murah juga maklumat salah (disinformation) boleh diedarkan tanpa sekatan dan halangan, umpama 'lalang kering yang terbakar ditiup angin'. Kaedah penyebaran bahan terbitan elektronik telah digunakan iaitu melalui e-mel dan *'newsgroup'*. Didapati proses pertukaran maklumat di kalangan penggiat ruang siber sentiasa pesat, maka sesuatu berita (walaupun palsu) sangat mudah tersebar meluas. Misalnya insiden penyebaran berita 'Persediaan Keganasaan di Chow Kit' adalah bukti yang sangat jelas. Sebaik

[14] South China Morning Post, *"A Dissident Continue E-Mail Activity Despite Court Order"* 2th February, 1999

sahaja terpapar berita berkenaan di *newsgroups*[15], keadaan separa anomik telah terbentuk, sehinggakan ada sesetengah pihak mula mengambil langkah berjaga-jaga, misalnya mendapatkan bekalan makanan dan senjata kononnya sebagai langkah untuk menghadapi keadaan kacau bilau.

Ini membuktikan penerbitan elektronik di ruang siber bukan sahaja mudah, malahan boleh dikatakan hampir semua orang mampu menyempurnakannya. Pada masa yang sama penerbitan sedemikian berupaya menjangkau jumlah pembaca yang tanpa batasan (terutama sekali jika penerbitan berkenaan menggunakan bahasa Inggeris).

Ketika berlakunya konfik di Kososvo kegiatan penerbitan berbentuk digital di ruang siber memainkan peranan yang sangat besar. Ketika itu stesen Radio B92, bertindak menyalurkan berbagai maklumat dan siaran berita ke Internet dan diedarkan dalam bahasa Serb secara digital.

Di Malaysia penerbitan digital di ruang siber amat ketara sekali selepas September 1998. Berpuluh-puluh laman-web dibangunkan semata-mata untuk menyiarkan 'maklumat' yang tidak dapat diperolehi dari akhbar-akhbar arus perdana. Berbagai bentuk penerbitan dibuat semata-mata untuk menjayakan usaha-usaha menyebarkan maklumat seluas mungkin. Pada masa itu permintaan terhadap bentuk-bentuk penerbitan yang seumpama ini sangat

---

[15] Antara *newsgroups* yang popular ialah *soc.culture.malaysia*

tinggi dan popular seperti Laman Reformasi[16], Saksi, Harakah Daily dan sebagainya. Begitu juga kelahiran akhbar digital seperti "Malaysiakini" adalah kerana wujudnya permintaan untuk yang seumpamanya. Pada ketika itu jumlah pengguna Internet yang mendaftar dengan pembekal khidmat Internet (Internet Service Provider - ISP) telah meningkat dengan pesat dan diakui oleh ISP tempatan[17].

Sungguhpun terdapat halangan atau sekatan ke atas penggunan Internet di sesetengah negara tetapi hal ini tidak berlaku di Malaysia Pada masa yang sama, apabila kerajaan Yugoslavia cuba mengawal berita dari Internet, didapati adanya usaha yang bertujuan mengatasi sekatan berkenaan. Sehubungan itu *Kosovo Privacy Project* telah diperkenalkan oleh *Anonymizer Inc*[18] yang menyediakan laman web bagi tujuan 'melindungi' mereka yang ingin melayari web yang dianggap sensitif dan akan dapat mengelakkan diri dari dikesan[19]. Oleh itu semua maklumat sama ada melayari laman web atau penghantaran e-mel yang menggunakan perkhidmatan ini 'tidak akan dapat dikesan' melalui kaedah biasa seperti *net-scanning* atau melalui kaedah menjanakan semula jejak digital yang biasanya boleh diperolehi dari log fail pengguna. Selain dari itu

---

16 Laman Reformasi pernah menjadi antara laman-web paling popular di dunia, dengan trafik permintaan melebihi 10,000 sehari.

17 Walau bagaimanapun data terperinci tidak dapat dikemukakan, ISP seperti TM-Net (merupakan pembekal laluan Internet yang terbesar di Malaysia) mengalami peningkatan jumlah pengguna baru.

18 Dicapai melalui www.anonymizer.com

19 Kaedah yang digunakan adalah untuk menghapus *'digital-trail'*

tidak meninggalkan *history* di pelayan Internet mahupun juga di komputer yang digunakan untuk melayari web (Fiery, 1994).

Disebabkan kandungan bahan penerbitan mereka banyak menyentuh berbagai perkara yang dianggap bertentangan dengan undang-undang, kehadiran bahan-bahan berkenaan sudah tentu akan menimbulkan masalah yang sangat besar untuk diatasi. Antara bahan-bahan yang diterbitkan dan mudah dicapai melalui Internet menerangkan tentang cara untuk menggodam (hacking) sistem komputer (Meinel, 1998) terutama sekali yang berkaitan dengan perisian operasi *Microsoft Windows*™ dan perisian *Microsoft Office Suite*™. Di samping itu dijelaskan cara-cara memanipulasi perisian yang lain, mengeksploit, memecah masuk katalaluan (password cracking) dan perkara-perkara lain yang boleh menjejaskan kestabilan perisian berkaitan.

Di kalangan siber-teroris pula, mereka berminat menggunakan Internet bagi memboleh mereka menyampaikan berbagai makluman dan maklumat penting mengenai kegiatan yang mereka jalankan (Guisnel, 1997). *Emergency Response & Research* (yang berpengkalan di Chicago, Amerika Syarikat) telah menyatakan dalam maklum-balas kepada Jawatankuasa Senat Amerika Syarikat: terdapat banyak pertubuhan pengganas di dunia menggunakan Internet dalam usaha menyebarkan maklumat mereka. Dari sebesar-besar organisasi seperti Hizbollah (www.hizbollah.org) hinggalah ke *Liberation Tigers of Tamil Eelam* dan pertubuhan-pertubuhan lain yang kecil, termasuk juga Gerakan al-Maunah di

Malaysia, yang mempunyai laman-webnya sendiri[20] untuk mewar-warkan perjuangan mereka.

Dialog – Ruang siber juga menjadi medan perdebatan yang terbesar melalui kaedah e-mel, *newsgroups*, *chat* dan *web-forum*. Secara umum dialog boleh dibahagi kepada dua jenis utama iaitu yang terhad kepada ahli yang berdaftar atau yang terbuka untuk semua orang. Kegiatan seumpama ini turut disediakan oleh organisasi berita seperti CNN yang memberi ruang kepada pembaca untuk memberi maklum-balas terhadap berita yang disiarkan. Tidak ketinggalan juga terdapat organisasi kerajaan dan bukan kerajaan yang menyediakan platform bagi membolehkan semua pihak turut serta dalam diskusi-maya. Tambahan pula proses penyediaan laman-dialog begitu mudah dilakukan dan sebahagian besarnya adalah percuma.

Terdapat berpuluh-puluh laman web yang mengkhusus kepada kegiatan seumpama ini. Sebagai contoh, perisian komunikasi ICQ[21], iaitu sejenis perisian yang disediakan oleh syarikat yang berpengkalan di Israel yang telah berjaya menghimpunkan lebih dari 10 juta keahlian. Seringkali perbincangan maya melibatkan hampir berbagai jenis isu yang meliputi politik, ekonomi dan

---

[20] http://RVL4.ecn.purdue.edu/~cromwell/lt/terror.htm - terlampir senarai pertubuhan 'pengganas' yang memiliki laman web.

[21] Boleh didapati di www.ICQ.com, di samping itu terdapat juga perisian yang seumpamanya seperti Yahoo.com dan MSN

sosial. Di kalangan *hacktivism*, mereka gemar dengan perbincangan tentang isu *privacy* dan hak[22].

Di Malaysia, terdapat juga bentuk dialog seumpama yang wujud seperti alternatif-net, keadilan-net dan sangkancil-net yang dianggap sebagai platform utama untuk kalangan aktivis politik pembangkang berdiskusi. Sungguhpun kegiatan perbincangan tidak melibatkan kalangan pimpinan tertinggi dan utama parti-parti politik tetapi dari semasa ke semasa terdapat juga *posting* langsung dari mereka. Berbagai perkara yang dibincangkan termasuk isu-isu dan tindakan-tindakan kerajaan, komen dan kritik sering disiarkan untuk tatapan aktivis (politik khususnya) dan turut terbabit secara aktif dalam perbincangan (Strassmann, 1995).

Koordinasi – kegiatan di kalangan aktivism amat bergantung kepada ruang siber. Keupayaannya yang efisyen dan murah menjadikan banyak pihak yang memiliki apa jua kepentingan pasti akan menggunakan ruang siber sebagai platform koordinasi kegiatan mereka. Tidak ada cara yang lebih cekap, cepat dan murah yang dapat mengatasi kaedah ini. Sebarang aktiviti boleh dimaklum dengan mudah melalui e-mel, ahli hanya menunggu setiap pengumuman mengenai kegiatan yang ingin dijalankan. Malahan tiada sempadan masa dan geografi yang boleh menghalang usaha mengkoordinasi dijalankan.

---

22 *Newsgroups* utama seperti *alt.privacy* dan *sci.crypt*

Protest.net menyediakan satu ruang khusus kepada aktivis-aktivis untuk mengumumkan, melaporkan, mengkoordinasi semua jenis kegiatan mereka seperti makluman tempat dan masa serta propaganda yang mereka jaja. Begitu juga untuk mengendalikan kegiatan mereka seperti mesyuarat perjumpaan dan lain-lain. Secara tidak langsung permasalahan logistik dan kos yang perlu ditanggung oleh pihak yang terlibat bukan saja dapat dikurangkan tetapi juga menjadi lebih cekap.

Kekuatan Internet memobilisasikan penyokong telah dibuktikan dari berbagai insiden sama ada yang berlaku di luar negara atau dalam negara. Sebagai contoh, apabila pihak agensi perisikan Turki berjaya menangkap Abdullah Ocalan[23], maklumat berkenaan telah tersebar dengan meluas dalam jangkmasa yang singkat. Pergerakan pro-Kurdish telah bangkit dan mengadakan bantahan. Ini membuktikan kehadiran Internet telah mencorak semula bagaimana kegiatan politik mewujudkan hubungan (alliance) dan pemuafakatan seperti yang diperjelaskan oleh Prof Dartnell, *Concordia University.*

Dalam persidangan G8 di Cologne, Germany pada 18 Jun 1999, satu koordinasi siber dan fizikal secara besar-besaran telah dijayakan. Kegiatan kali ini bukan sahaja dilakukan melalui protes jalanan sebagaimana selalu, tetapi juga serangan *'hacking'* dilakukan ke atas lebih 20 organisasi perniagaan dan

---

[23] Tokoh pimpinan utama dalam Gerakan Pembebasan Kurdish

perdagangan utama dunia. Gabungan *hackers* dari Indonesia, Israel, Germany dan Canada telah melancarkan gerakan selama lima jam terhadap organisasi korporat termasuk *Barclays Bank* dan *London Stock Exchange.*

Gerakan *The International Campaign to Ban Landmines* adalah gabungan tidak kurang 1,300 pertubuhan di 75 negara. Mereka juga menggunakan ruang siber bagi mempengaruhi polisi terhadap penghapusan periuk api. Kegiatan kempen meliputi penghapusan penggunaan, pengeluaran, simpanan stok, dan penjualan atau pemindahan periuk api dan memusnah periuk api. Liz Bernstein salah seorang aktivis bagi tujuan anti-periuk api berpendapat bahawa, penggunaan Internet telah mempercepatkan proses memperolehi sokongan dari pelbagai negara. Usaha yang dimulakan pada 1996 akhirnya berjaya dicapai apabila mulai 1hb March 1999, satu undang-undang melalui konvensyen antarabangsa menyekat penggunaan periuk api diluluskan dan sehingga kini 135 negara telah menandatangani perjanjian berkenaan. Ini adalah bukti jelas tentang keupayaan ruang siber yang mampu untuk mempengaruhi polisi negara melalui usaha koordinasi yang dijalankan melalui Internet.

Di Malaysia, kegiatan golongan atau aktivis reformasi amat bergantung kepada kehadiran Internet. Sejak dari insiden 20hb September 1998, di Dataran Merdeka, Kuala Lumpur, telah banyak aktiviti-aktiviti diwar-warkan melalui Internet. Peristiwa demontrasi jalanan dari siri "Membeli-belah di

Hujung Minggu" pada tahun 1998, sehingga membawa kepada peristiwa tahunan "*The Black 14*" kepada insiden "Perhimpunan 100,000 Rakyat", semuanya digembelingkan melalui Internet. Maklumat disiarkan secara meluas di laman-lawan web pro reformasi[24], berbagai bentuk maklumat dan aktiviti diperjelaskan kepada penyokong-penyokong kelompok ini. Salah satu dari kaedah yang sering dijalankan ialah dengan menyebarkan poster secara elektronik dan. (Sila lihat contoh poster edaran yang diperolehi dari laman web pro-reformasi.)

Hacktism – gerakan jenis ini sedikit berbeza dengan cara dan kaedah yang sering digunakan oleh aktivism, kerana langkah yang sering diambil lebih banyak berlawanan dengan undang-undang yang sedia ada. Kegiatan mereka yang telah dikenalpasti seperti *electronic civil disobedience*; *virtual sit-ins*, halangan (blockade), *e-mail bomb*, hacking, penghantaran trojan, virus dan *worms*[25](Schwartau, 1995).

Virtual sit-ins & Blockade: Tindakan *virtual sit-ins* dan halangan dilakukan ke atas laman-laman web. Di dapati pernah berlaku ke atas laman-laman web milik agensi-agensi kerajaan Perancis menerima tindakan seumpama ini kerana memprotes terhadap polisi nuklear dan lain-lain polisi sosial negara berkenaan. Ini terbukti pada 21 Disember 1995 satu tindakan yang dianjurkan oleh *Strano*

---

[24] Laman-laman web ini diwujudkan sebagai tanda sokongan kepada perjuangan reformasi yang dipelopori oleh Datuk Seri Anwar Ibrahim.

[25] Sila rujuk Lampiran II, ms viii.

Network, ialah meminta supaya semua *hacktivist* dari seluruh dunia yang terlibat melancarkan *browser* ke alamat laman-laman web yang ditetapkan selama satu jam[26].

Tindakan yang lebih besar dilakukan oleh kumpulan *Electronic Disturbance Theater (EDT)*, langkah yang dijalankan lebih tersusun dan berkesan. Bagi menjayakan tindakan ini, semua yang terlibat diminta melayari laman *FloodNet* dan mendapatkan perisian yang boleh dibeban-turun (download) dan menjalankan *(execute)* perisian berkenaan. Mereka dibenarkan untuk memasukkan kenyataan seperti *"human_rights not found in this server"*. Oleh kerana perisian ini dijalankan secara otomatik, maka pelayan web yang menjadi sasaran akan merekodkan kenyataan protes yang dilakukan oleh kelompok berkenaan secara bertalu-talu. Mengikut anggaran 10,000 orang yang terlibat dengan kegiatan ini yang menyebabkan 600,000 hits seminit seperti yang telah direkodkan di pelayan web berkenaan. Serangan yang seumpama ini pernah dilakukan ke atas pelayan web Pentagon, Presiden Zedillo Mexico dan Bursa Saham Frankfurt.

E-Mail Bomb: Tindakan yang dijalankan walaupun lebih mudah (dengan tujuan semata-mata untuk menarik perhatian ke atas pihak yang menjadi sasaran mereka) tetapi mempunyai kesan yang besar. Dengan menghantar e-

[26] Terdapat laporan yang menyatakan tindakan yang seumpama ini telah mengakibatkan pelayar-web terhenti atau terjejas.

mel kepada sasaran secara berulang-ulang pada satu-satu jangka masa setiap hari atau dalam jangkamasa yang ditetapkan. Namun apabila e-mel yang dihantar dalam jumlah ribuan akan mengakibatkan pelayan e-mel yang disasarkan akan terjejas. Penggunaan kaedah ini bertujuan memprotes, mengganggu berkali-kali (harassment) dan balas dendam.

Pihak perisikan U.S. telah merekodkan tindakan yang seumpama ini yang dilakukan oleh kumpulan *Liberation Tigers of Tamil Ealam.* Mereka telah bertindak dengan menghantar *e-mail bomb* ke pejabat-pejabat kedutaan Sri Lanka dengan kandungan e-mel mereka *"We are the internet Black Tigers and we're doing this to distrupt your communications"*[27], jumlah e-mel yang dihantar sebanyak 800 e-mel sehari.

Sewaktu pertelingkahan di Kosovo memuncak, *e-mail bombs* turut digunakan oleh kedua-dua belah pihak. Rekod telah menunjukkan selepas *The Belgrade Hackers* menyerang pelayan web milik NATO dengan menghantar sebanyak 2,000 e-mel sehari, mereka kemudiaannya menerima tindakbalas dari Richard Clark (penduduk di California) menghantar 500,000 e-mel ke pelayan e-mel kerajaan Yugoslavia hingga menyebabkan lumpuhnya pelayan e-mel dan web berkenaan.

---

[27] "A e-mail attack on Sri Lanka Computer" Computer security Alert, No. 183, Computer Security Institute, June 1998

Gambaran ini menunjukkan kekuatan ruang siber yang digunakan sebagai alat untuk bertindak dan bertindakbalas ke atas sesuatu sasaran. Keadaan ini juga menunjukkan bagaimana kemampuan ruang siber boleh digunakan untuk tujuan positif dan juga negatif.

Menggodam Laman Web & Komputer: Satu lagi bentuk yang amat popular yang digunakan oleh golongan *hacktivism* (Northcutt, 1999). Langkah ini disifatkan lebih kepada usaha untuk meruntuhkan sesuatu laman web yang menjadi sasaran. Seringkali tindakan ini akan mengakibatkan berlakunya tindak balas yang mungkin mencetuskan '*cyber-war*' (Wolff, 1996).

Satu insiden di Indonesia yang pernah berlaku apabila seorang penggodam dari Portugis, yang bertindak memecah masuk ke pelayan web kerajaan Indonesia dan meminda kandungannya dengan memasukkan mesej *"Free East Timor"*. Di Malaysia, juga pernah gempar apabila laman-web Parlimen dan beberapa universiti tempatan telah digodam dengan cara yang sama. Begitu juga tindakan ke atas laman web milik kelompok pro-reformasi yang popular telah dipinda dan digantikan dengan gambar lucah oleh kumpulan penggodam anti-reformasi.

Cyberterrorism: Apabila gerakan terroris bergabung dengan alam siber akan melahirkan kelompok ini. Istilah ini mula diperkenalkan oleh Barry Collin[28] disekitar 80an, dan Mark M. Pollitt memberikan definisi sebagai;

> *"cyberterrorism is pre-meditated, politically motivated attack against information, computer system, computer program, and data which in result in violence against noncombatant targets by sub national groups or clandestine agents[29]"*

Didapati internet juga turut dimanfaatkan oleh pengganas atau teroris untuk kepentingan pihak mereka (Olson-Raymer, 1996). Propaganda yang diedarkan secara digital membuktikan kehadiran golongan ini di ruang siber. Walau bagaimanapun, kemampuan kelompok ini melakukan serangan secara *cyberterrorism* belum dapat dibuktikan secara empiris (Denning, 1999). Namun kemungkinan berlakunya perkara ini di masa depan adalah tidak dapat dinafikan. Pihak perisikan Amerika Syarikat berpendapat tindakan *Tamil Tigers* melalui *e-mail bombs* adalah bukti yang menunjukkan potensi berkenaan boleh berlaku. Kemampuan hackers seperti Kevin Matnick[30] menyelinap masuk dalam sistem komputer yang diklasfikasikan sebagai sensitif dan berkeselamatan tinggi membuktikan situasi yang sama boleh berlaku, yang memungkinkan wujud gerakan *cyberterrorism* akan menjadi ancaman di masa

---

[28] Ketika itu beliau adalah Senior Fellow di Institute for Security and Intelligence, California

[29] "Cyberterrorism: Fact and Fancy": Proceeding of the 20th National Information System Security Conference, October 1997. Pp 285-89

[30] Kevin Matnick – bukan seorang cyberterrorist, beliau adalah salah seorang hacker yang terkenal dan telah dikenakan hukuman penjara pada tahun 2000, kini telah di bebaskan.

depan (Shimomura & Markoff, 1996). Pollitt[31] pula berpendapat pada masa akan datang kemampuan *cyberterrorist* berupaya bertindak dan meninggalkan implikasi lebih teruk berbanding dengan serangan bom yang pernah dilakukan pada masa-masa yang lalu.

Sungguhpun pada masa ini belum lagi berlaku sebarang kejadian serius dan mengancam keselamatan akibat dari tindakan kelompok ini tetapi penilaian terhadap kemungkinan berlakunya situasi ini harus dianggarkan dengan lebih teliti. Tetapi telah terbukti terdapat beberapa peristiwa yang boleh dianggap sebagai kejadian tahap pertama kepada merealitikan gerakan cyberterrorism. Mengikut laporan Senat Amerika Syarikat, terdapat beberapa pertubuhan pengganas terutama di Asia Barat sedang berusaha untuk membentuk rangkaian *hackers* yang bertujuan memperolehi perisian keselamatan (security software) ketenteraan bagi membolehkan mereka melancarkan *information warfare attack* (Denning, 1999).

3.2 Realiti Ancaman e-jenayah

Maka jelas terbukti bahawa kehadiran Internet telah menyediakan ruang yang cukup baik untuk sesetengah golongan yang bertujuan menyempurnakan tindakan e-jenayah. Berbagai perlakuan dapat dilakukan oleh golongan ini,

[31] Mark M.Pollitt "Cyberterrorism: Fact and Fancy": Proceeding of the 20th National Information System Security Conference, October 1997. Pp 285-89

termasuk memanipulasi untuk tujuan penipuan (fraud)[32], penjualan dan pengedaran pornografi kanak-kanak, penjualan senjata dan dadah terkawal, pengedaran perisian komputer yang diciplak dan lain-lain bahan kreatif secara haram. Dalam keadaan yang lebih ekstrim lagi apabila adanya perlakuan jenayah seperti *cyber-stalking*, menceroboh sistem rangkaian komputer melalui Internet, memperolehi maklumat dari sistem yang dicerobohi, hingga menjejaskan intergriti sistem rangkaian komputer dan perlakuan lain yang dianggap menyalahi undang-undang (Cheswick, 1994).

Oleh itu adalah menjadi tanggungjawab semua pihak khususnya di Malaysia seperti penggubal undang-undang (legislator), pembentuk polisi, organisasi yang terbabit langsung dan tidak langsung dengan industri komputer dan pihak penguatkuasa mengambil kira peningkatan perlakuan e-jenayah yang dijangka selari dengan perkembangan dan pertumbuhan penggunaan Internet pada masa kini dan akan datang. Jika tidak maka harapan untuk menjadikan Malaysia sebagai hub teknologi maklumat yang terulung di rantau Asia Tenggara khususnya mungkin akan terjejas akibat tindak-tanduk perlakuan e-jenayah[33].

Secara umum terdapat berbagai usaha yang bersungguh-sungguh untuk memperkenalkan pelbagai polisi dan juga undang-undang yang berkaitan

---

[32] Sila rujuk Lampiran V, ms xvii – bagi penjelasan lanjut tentang kegiatan penipuan.

[33] National Research Council (1991) *Computer at Risk: Safe Computing in the Information Age*. Washington, D.C., National Academy Press.

selaras dengan kemajuan dan peningkatan keupayaan teknologi pengkomputeran dan Internet. Namun, kita masih belum dapat menjangkakan sejauhmana tahap dan kemampuan jenayah komputer atau jenayah berkaitan dengan komputer (di Malaysia) dalam jangka masa terdekat mahupun di masa akan datang (Rosenoer, 1997). Sehingga setakat ini insiden e-jenayah yang sering berlaku ialah tindakan mencacatkan laman-laman web tempatan. Tiada terdapat kejadian menggodam yang serius hingga melumpuhkan komputer berkenaan dilaporkan. Insiden yang seumpama ini pernah berlaku pada tahun 2001 iaitu laman web milik kerajaan seperti Parlimen Malaysia (www.parlimen.gov.my) dan Universiti Teknologi Malaysia (www.utm.edu.my) telah 'dipadamkan' oleh penggodam.

Adalah dipercayai terdapat juga insiden-insiden e-jenayah yang lebih serius termasuk tindakan mencerobohi atau cubaan untuk mencerobohi rangkaian sistem komputer milik organisasi tempatan, tetapi tiada laporan rasmi dibuat. Oleh yang demikian amat sukar untuk pihak kerajaan khususnya menjangkakan tahap sebenar potensi ancaman e-jenayah ke atas negara secara umumnya. Hal ini disebabkan kegagalan organisasi persendirian dan perniagaan terutamanya untuk memaklumkan atau menyatakan secara terbuka kepada pihak berkuasa tentang kejadian atau insiden jenayah komputer yang

membabitkan organisasi mereka[34]. Perkara ini diakui sendiri oleh Menteri di Jabatan Perdana Menteri, Datuk Seri Rais Yatim. Menurut beliau seringkali organisasi berkenaan lebih bersikap membisu mengenai kejadian berkenaan. Jika ada pun laporan dibuat perkara berkenaan hanya dimaklumkan kepada pihak-pihak tertentu sahaja yang berkaitan dan tidak kepada pihak berkuasa tempatan.

> *"We can understand that but what we are saying is that the criminal part of the job must be shared because there is no telling when a company can be hacked,"*[35]

Seharusnya sektor swasta tampil ke hadapan memaklumkan perkara berkenaan dan turut berkongsi maklumat. Di samping sektor tersebut harus turut membantu dengan cara berkongsi teknologi enkripsi (encryption) dengan pihak lain bagi membolehkan mereka yang terbabit menerima manfaat atau nasihat melindungi rangkaian sistem komputer mereka dari ancaman 'luar'. Perkara yang serupa pernah disentuh oleh Timbalan Perdana Menteri, Dato' Seri Ahmad Badawi yang meminta kerjasama penuh daripada semua pihak untuk membantu pihak penguatkuasa[36]. Tambah beliau lagi pencegahan melalui undang-undang tidak akan berjaya tanpa kerjasama yang baik dari orang ramai.

---

[34] Sila rujuk Lampiran 1: Contoh borang untuk mengemukakan laporan mengenai insiden e-jenayah kepada *MyCert.*

[35] Sewaktu Dr Rais bercakap kepada pemberita selepas menyampaikan ucaptama beliau sewaktu merasmikan *2001 Emergency Response Planning Conference* at the Maktab Pegawai-Pegawai Polis, pada 23hb Oktober, 2001, dipetik dari agensi berita BERNAMA

[36] Petikan ucapan sewaktu merasmikan pelancaran NISER – *National ICT Security and Emergency Response* pada 10hb April 2001.

Di pihak pendakwa raya pula amat perlu baginya dari semasa ke semasa mengkaji dan menilai semula peruntukan undang-undang yang sedia termasuk meminda mana-mana bahagian yang perlu, terutama sekali yang berkaitan dengan prosedur penyediaan bahan bukti dan keterangan, bagi tujuan pendakwaan kes-kes e-jenayah atau jenayah yang ada kaitan dengan komputer[37]. Ini kerana memang diakui bahawa peruntukan undang-undang yang sedia didapati belum lagi memadai dan perlu dipinda mengikut peredaran kemajuan ICT.

Undang-undang yang terdapat di Malaysia, khususnya Undang-undang Keterangan, mendefinisikan komputer sebagai;

> *"... any device for recording, storing, processing, retrieving or producing any information or any matter, or for performing any one or more of those functions, by whatever name or description such device is called; where two or more computers carry out any or more of those functions in a combination or in a succession or otherwise howsoever conjointly, they shall be treated as a single computer."*[38] *(section 3 – Interpretation: Evidence Act)*

Sungguhpun begitu, Dr. Rais sendiri mengakui bahawa adalah menjadi keperluan utama pada masa kini untuk para pendakwaraya menguasai kemahiran yang berkaitan dengan teknologi pengkomputeran dan teknologi maklumat bagi membolehkan mereka menyempurnakan tanggungjawab mereka dengan lebih baik. Hal ini memandangkan penguasaan kemahiran ini sudah menjadi satu keperluan dan bukan lagi suatu tugas yang boleh dipandang

---

37 _____ (2001) *Prosecuting Cases that Involve Computer: A Resource for State and Local Prosecutors.* National White Collar Crime Center, 2001.

38 Effective from July 15th 1993, Evidence (Amendment) Act 1950 (A851) 1993

enteng. Penguasaan kemahiran secara komprehensif dalam pengendalian pengkomputeran dan perkakasan yang berkaitan akan dapat membantu mereka di m` ahkamah. Misalnya, mengemukakan kandungan cakera-keras (hard disk) sebagai bahan bukti sewaktu mengemukakan keterangan untuk menunjukkan perlakuan jenayah telah berlaku (Rosenblatt, 1996). Jika pihak pendakwa tidak memiliki kemahiran khusus terutama dari segi pengendalian, bahan bukti yang diperolehi mungkin 'musnah' kerana sifatnya yang sensitif.

Keadaan ini menunjukkan bahawa perlu adanya usaha untuk menilai semula paradigma perundangan yang sedia ada supaya sejajar dengan kehendak perubahan teknologi maklumat itu sendiri. Seperti mana pesatnya perubahan masyarakat pada masa ini disebabkan kemajuan teknologi maklumat, maka keupayaan perlaksanaan dan amalan undang-undang seharusnya juga menepati kehendak yang serupa dan tidak seharusnya bersifat statik dan arkaid (archaic). Dengan kata lain, undang-undang yang sedia ada harus berubah selari dengan peredaran kemajuan teknologi masa kini (Parker, 1998).

BAB 4

4. Komputer & Internet: modus operandi e-jenayah

Dalam masyarakat yang pesat berkembang terutama sekali hasil didorong oleh kemajuan teknologi komputer, permasalahan utama yang terpaksa dihadapi ialah berkaitan jenayah komputer yang kini semakin menjadi-jadi. Boleh dikatakan kepesatan perubahan teknologi meninggalkan kesan yang ketara dalam berbagai aspek kehidupan misalnya dari segi sosio-ekonomi seharian; sistem perbankan dan perdagangan. Dalam hal ini penyediaan prasarana digital seolah-olah turut memberi ruang kepada golongan yang mungkin mengeksploit sistem prasarana berkenaan bagi kepentingan diri (Garfinkel & Spafford, 1997).

Pada hari ini jenayah yang melibatkan komputer adalah dianggap sebagai sebahagian daripada *economic criminality*, iaitu menggambarkan bahawa perlakuan berkenaan sering berlaku. Oleh itu sistem komputer yang terdapat di bank, firma perdagangan dan sektor industri yang dianggap memiliki nilai ekonomi yang tinggi mempunyai risiko akan 'diserang' oleh golongan e-jenayah. Tindakan yang mungkin akan mereka lakukan ialah mencuba 'masuk' (intrude) ke dalam sistem maklumat berkenaan memperolehi sebarang maklumat yang berharga bagi tujuan kegunaan tertentu (Martin, 1998).

Terdapat juga yang akan bertindak memanipulasi sistem maklumat yang sedia ada termasuk meminda program atau perisian yang terdapat di sana bagi tujuan sesuatu kepentingan yang lain. Mereka juga mungkin bertindak memasukkan maklumat palsu atau mengemukakan sesuatu arahan tanpa izin (unathorized instructions) terhadap sistem berkenaan semata-mata bagi mendapatkan imbuhan khususnya dari segi wang (Northcutt, 1999). Gambaran seperti ini dapat disaksikan dalam satu filem cereka bertajuk *"Swordfish"*. Dalam filem tersebut segolongan pelaku jenayah telah berjaya merencana satu usaha memindahkan sejumlah wang dengan cara manipulasi yang kompleks terhadap sistem maklumat bank. Di Malaysia insiden yang pernah berlaku pada tahun 2000 dan 2002, apabila terdapat sekumpulan e-jenayah yang menggunakan kaedah *skimming* untuk mengklon kad ATM[39] dan kemudiannya melakukan pengeluaran melalui ATM.

Maka jelaslah teknologi komputer tidak hanya menyumbang ke arah perubahan positif masyarakat dalam pelbagai urusan hari, tetapi juga turut menyediakan ruang bagi membolehkan seseorang itu mengendalikan urusan yang melanggar undang-undang. Dengan kata lain perubahan yang berlaku terhadap kehidupan masyarakat tidak hanya bersifat kuantititatif tetapi juga turut melibatkan perubahan kualitatif. Misalnya dalam penggunaan e-mel pada hari ini, sama seperti penggunaan surat dalam sistem perhubungan

[39] Rujuk laporan The Star 16 April 2000 dan 23 June 2002.

konvensional yang menyediakan mekanisma untuk menghantar mesej kepada seseorang. Tetapi keupayaan e-mel bukan hanya sekadar mampu untuk menghantar mesej sahaja tetapi juga fail/dokumen/program perisian kepada mana-mana pihak di mana-mana jua dalam pelbagai format seperti *audio-visual.* Namun begitu yang menjadi soalan ialah sejauhmanakah keupayaan sistem berkenaan mampu melindungi penggunanya (pengirim atau penerima) dari pihak-pihak lain yang mungkin berjaya memintas e-mel berkenaan dan memperolehi maklumat yang terkandung di dalamnya. Dalam hal yang lain e-mel juga boleh digunakan untuk menjalankan aktiviti jenayah seperti kegiatan penyebaran gambar-gambar pornografi dan kegiatan pedofil[40].

Dalam era teknologi maklumat dan pengkomputeran yang canggih ini sudah pastilah pelaku jenayah akan sentiasa melengkapkan diri mereka dengan berbagai pengetahuan untuk mempertingkatkan kecekapan mereka bagi menjayakan aktiviti-aktiviti jenayah. Ini kerana pengetahuan yang seumpama itu mampu membantu mereka menjadikan komputer sebagai peralatan yang sangat berkuasa untuk mempasti atau menjaminkan kejayaan mereka dalam kegiatan berkenaan. Oleh itu, bagi memahami dengan lebih lanjut tentang dan bagaimana keupayaan sesuatu komputer dan kemampuan pelaku jenayah dalam kegiatan mereka. Maka amat penting sekali untuk memiliki pengetahuan khusus mengenai penggunaan komputer dan bagaimana dapat digunakan bagi

[40] U.S. Department of Justice (2001) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Washington D.C.

tujuan jenayah (Davis, 1991). Tanpa pengetahuan yang mendalam mengenai komputer dan kemampuannya, pihak penguatkuasa sudah pasti tidak akan mampu memenuhi kehendak dan cabaran yang berkaitan dengan perlakuan jenayah komputer itu sendiri.

Secara umum komputer boleh berperanan dalam kegiatan jenayah melalui tiga cara berikut;

4.1.1 Komputer sebagai Sasaran

Salah satu tindakan pelaku jenayah komputer adalah menjadikan komputer sebagai sasaran utama mereka. Berlakunya situasi ini adalah berpunca dari tindakan (serangan) untuk memperolehi maklumat yang terkandung di dalam sistem pengkalan data. Antara tindakan yang sering dilakukan ialah melaksanakan serangan ke atas sesuatu sistem komputer dan cuba untuk mendapatkan maklumat melalui proses muat-turun (download) secara kawalan-jauh (remote-access). Kaedah ini seringkali dilakukan dengan cara menceroboh (intrusion) masuk tanpa kebenaran atau bayaran - diistilahkan sebagai *theft of service* - dan diikuti dengan tindakan meminda atau mengganggu gugat (interfere) pelayan komputer (computer-server) bertujuan menjejaskan operasi komputer (National White Collar Crime Center, 1999). Perlakuan yang seumpama ini disebut juga sebagai kaedah menggodam atau *hacking*.

Akibatnya konfidentialiti, intergriti atau maklumat yang dimiliki oleh sesuatu komputer akan terjejas atau tercabar (compromise). Selain dari itu serangan ke atas sistemnya kemungkinan akan lumpuh sistem komputer berkenaan. Tindakan mendapatkan maklumat atau mencuri maklumat berlaku dalam berbagai bentuk bergantung kepada keadaan peranan sistem komputer yang dicuri masuk. Sekiranya rangkaian sistem komputer yang dicuri masuk itu menyimpan maklumat sensitif misalnya milik pihak penguatkuasa keselamatan atau tentera (seperti di Amerika Syarikat sistem rangkaian komputer milik Biro Penyiasatan Persekutuan – FBI- dan Agensi Angkasalepas Kebangsaan – NASA- sering menjadi sasaran penggodam) maka kemungkinan terjejas keselamatan negara akan berlaku. Ini kerana ramai bertanggapan kandungan maklumat yang terkandung didalamnya mempunyai nilai strategik dan ekonomi yang tinggi (Mc Carthy, 1998). Oleh itu tindakan menggodam sistem komputer seumpama itu mungkin akan 'menarik' organisasi jenayah terancang, organisasi pengganas mahupun juga agensi perisikan asing.

Di samping itu rangkaian komputer milik organisasi bukan kerajaan, perdagangan ataupun perniagaan turut juga menjadi sasaran pelaku e-jenayah semata-mata untuk memperolehi maklumat bernilai seperti nombor kad kredit, yang digunakan tujuan pemalsuan atau

mengklon menipu bagi tujuan pembelian secara *online*. Di samping juga, untuk memperolehi perisian atau program komputer yang kemudian diedarkan atau dijual atau diedar tanpa kebenaran kepada mana-mana pihak yang berminat. Tindakan yang berbentuk sedemikian disebut juga sebagai *intellectual property theft* (Parker, 1983). Dalam tindakan yang lain, pelaku e-jenayah ada kalanya cuba mendapatkan maklumat peribadi dengan tujuan memalukan pemilik maklumat berkenaan atau dengan niat memeras (extortion) wang dari mangsa. Terdapat juga dilakukan untuk tujuan persaingan perniagaan (dengan mencuri maklumat rahsia perdagangan) dan tidak kurang ia dilakukan kerana ingin mencuba atau sekadar ingin tahu. Seringkali perlakuan seumpama ini membabit tindakan menggodam pelayan komputer sama ada milik sistem telekomunikasi seperti telefon, pengkalan data rekod perubatan dan pengkalan data yang lain bagi membolehkan mereka memperolehi berbagai jenis maklumat yang bernilai (Rusell et. al., 1992).

Dalam situasi yang lain pula, terdapat kegiatan di mana pelaku jenayah bertindak menceroboh masuk ke dalam sistem komputer telekomunikasi dengan tujuan memanipulasikan *telephone switching*

system untuk mencuri perkhidmatan panggilan jauh[41]. Wujud juga kegiatan seumpama ini yang membabitkan tindakan menceroboh masuk ke dalam sistem telekomunikasi 'kritikal' sehingga mungkin akan menjejaskan keselamatan pengguna yang lain seperti mencerobohi sistem telekomunikasi menara kawalan lapangan terbang atau sistem perkhidmatan kecemasan (Schulman, 1992).

Kegiatan menggodam juga berlaku apabila penggodam cuba memperolehi berbagai maklumat untuk menjalankan berbagai kegiatan pengkomputeran secara intensif, misalnya dalam usaha mendapat kata-laluan dari laman web yang lain. Kaedah yang digunakan dikenali sebagai *weaving*[42], iaitu bertindak menggunakan *resource* komputer yang lain sebagai batu loncatan untuk melancarkan serangan ke atas sistem rangkaian komputer yang lain (Slatalla, et. al., 1995).

Sejenis lagi bentuk serangan yang dilakukan secara kolektif disebut sebagai *'denial of service'* dengan objektif utama bukan untuk menceroboh masuk tetapi untuk melumpuhkan sistem komputer yang diserang. Tindakan ini dapat dicapai dengan melancarkan *'mailbombing'*, iaitu menghantar e-mel dalam jumlah yang besar secara serentak dan

---

[41] Kaedah ini dikenali sebagai *"phone phreaking"* atau *"phreaking."*

[42] Teknik yang membolehkan penggodam menggunakan beberapa rangkaian sistem komputer, Internet dan telekomunikasi (talian tetap dan talian telefon mudah-alih) dan dapat 'menghilangkan jejak' digital, identiti dan lokasi panggilan dibuat (Wolff, 1996).

bertubi-tubi ke satu alamat e-mel atau pelayan e-mel. Tindakan ini boleh dilakukan secara individu tetapi lebih berkesan jika dilakukan secara beramai-ramai. Akibatnya, pelayan-e-mel (e-mail-server) penerima akan dibebankan dengan penerimaan data yang banyak dalam masa yang singkat hingga mengakibatkan sistemnya lumpuh sama sekali dan tidak dapat berfungsi secara normal. Tindakan yang seumpama ini pernah berlaku kepada laman-web milik Yahoo.com, Amazon.com, eBay.com, CNN.com dan Buy.com hingga mengakibatkan laman-web ini terpaksa menggantungkan sementara perkhidmatannya untuk beberapa hari.

4.1.2 Komputer sebagai Alat Pengstoran

Kaedah kedua apabila komputer berperanan (dalam aktiviti jenayah elektronik) sebagai alat pengstoran maklumat atau data (Rusell et. al., 1992). Kemudahan yang ditawarkan oleh komputer hari ini adalah seperti maklumat boleh disimpan dengan mudah dan tersusun dengan menggunakan teknologi enkripsi *(encryption)* atau kriptografi *(cryptography)* (Denning, 1997). Kemudahan ini sudah tentu menarik berbagai pihak untuk menggunakannya, termasuk golongan penjenayah juga. Misalnya pengedar dadah mungkin menggunakan komputer untuk menyimpan berbagai jenis maklumat penting perniagaannya seperti bekalan, sumber, hasil jualan dan juga formula memproses

dadah. Contoh yang lain pula ialah apabila penggodam menggunakan komputer bagi menyimpan maklumat seperti kata-laluan, nombor kad kredit, maklumat *proprietary* mengenai sesuatu organisasi, imej pornografi dan perisian komersial yang diperolehi secara haram (dikenali sebagai *'warez'*) untuk berbagai kegunaan termasuk untuk diperdagangkan.

Pada masa yang sama kemampuan penyimpanan atau pengstoran dalam jumlah yang besar dan mudah dikendalikan membuktikan komputer boleh dijadikan sebagai pengkalan penyimpanan data atau maklumat yang efektif. Namun, dalam keadaan yang lain apa yang terkandung di dalam komputer berkenaan menjadi amat berharga kepada pihak berkuasa, terutama sekali untuk memperolehi bukti atau keterangan bagi tujuan pendakwaan. Tidak ketinggalan juga kehadiran komputer boleh mempertingkatkan keupayaan dan kemampuan pihak penguatkuasa untuk menghimpun maklumat atau keterangan yang dapat membantu untuk tujuan siasatan dan pendakwaan. Contoh maklumat rahsia yang dihapuskan (delete) dari sesuatu komputer tidak semestinya hilang begitu sahaja, dengan teknologi yang sedia ada usaha untuk mengembalikan maklumat berkenaan dapat dilakukan (berbanding dengan cara menghapuskan maklumat secara fizikal seperti membakar).

Situasi ini membolehkan segala keterangan diperolehi semula dan ini akan membantu mempercepatkan proses membuktikan kegiatan e-jenayah. Seringkali usaha untuk memperolehi semula atau mengembalikan maklumat atau bukti yang telah dihapuskan dengan sengaja oleh penjenayah (untuk tujuan tidak digunakan sebagai keterangan di mahkamah) memerlukan khidmat pakar forensik komputer, bagi mengembalikan maklumat yang 'dihilangkan' oleh penjenayah (Casey, 2000). Ini bermakna maklumat yang mungkin diperolehi sudah tentu akan dapat membantu dalam proses pendakwaan di mahkamah.

Sungguhpun begitu perlu diingatkan bahawa segala keupayaan dan kelebihan ini memerlukan pakar yang berkemampuan untuk membolehkan proses mengembalikan, mengumpul dan menghimpun maklumat itu. Seseorang ahli forensik komputer mestilah mahir dengan persekitaran sistem maklumat dan sistem rangkaian komputer yang digunakan. Jika tidak adalah tidak mungkin maklumat ini akan dapat diperolehi semula. Bagi pihak penguatkuasa dan pendakwa pula, mereka amat perlu memiliki pengetahuan yang mendalam dan khusus mengenai perkara yang berkaitan (Casey, 2000).

Di Malaysia, agensi seperti NISER mempunyai kepakaran bagi membolehkan usaha-usaha seumpama itu dijalankan. Berdasarkan

penyataan yang dikemukakan oleh Raja Azrina Raja Abdullah[43], NISER memiliki keupayaan mengembalikan maklumat yang hilang dari semua jenis komputer (sama ada komputer meja, komputer bimbit atau komputer telapak)[44].

4.1.3 Komputer sebagai alat Komunikasi

Komputer yang tersedia ada pada setiap pengguna adalah juga alat komunikasi yang cukup canggih dan serba lengkap. Ini memandangkan komputer terkini dilengkapi dengan kemudahan untuk dihubungkan dengan berbagai sistem rangkaian sama ada melalui *Local Area Network* atau *dial-up* yang membolehkan mereka dihubungkan dengan cekap ke rangkaian Internet intranet atau *extranet* (Ford et. al., 1997). Lebih-lebih lagi dengan kemudahan perkhidmatan jalurlebar (broadband) dan sistem komunikasi tanpa wayar (wireless) misalnya *Wireless Application Protocol* (WAP) dan kini sedang dipertingkatkan keupayaannya kepada *GPRS – 2.5G* –manakala tawaran tender untuk mengoperasikan tahap 3G telah dikeluarkan. Kemudahan ini membuka ruang kepada semua pengguna untuk melayari Internet biar di manapun mereka berada. Kepesatan pertumbuhan dan penggunaan Internet didapati sejajar dengan peningkatan penggunaan kemudahan yang

[43] Penolong Pengarah 1, NISER
[44] NST, Computimes 25 April 2002

serupa bagi membolehkan pelbagai perlakuan jenayah bersifat tradisional disempurnakan. Oleh itu hari ini banyak kejadian e-jenayah termasuk perlakuan jenayah tradisional mula dilakukan secara *online.* Paling minima komputer boleh digunakan untuk kegiatan jenayah sewaktu perancangan atau koordinasi sesuatu jenayah sebelum dilakukan sama ada secara *online* atau tidak (National White Collar Crime Center, 1999).

Penggunaan e-mel atau *real-time chat* pula memiliki kelebihan dari segi keupayaan berkomunikasi secara sulit (private), memberi kelebihan kepada pelaku jenayah untuk melakukan tindakan seperti mengugut, menyebar fitnah, malahan mengiklan berbagai jenis produk dan perkhidmatan yang melanggar undang-undang yang sedia ada. Sebagai contoh menjalankan skim cepat kaya secara piramid atau menjalankan perdagangan dadah secara *online.* Komunikasi berkomputer yang berlaku dalam format digital membolehkan perisian atau lain-lain (yang telah didigitalkan) dipindahkan secara mudah, murah dan cepat melalui kaedah muat-turun melalui *ftp* atau *http* (download). Oleh itu didapati tindakan seumpama ini begitu popular dilakukan sama ada secara sah atau juga tidak sah.

Penggiat pedofil sering menggunakan platform Internet bagi mengedar gambar-gambar pornografi kanak-kanak di samping itu menggunakan e-mel untuk berhubung dengan kanak-kanak bagi maksud yang seumpamanya. Begitu juga dengan tindakan penyebaran gambar-gambar lucah yang lainnya. Tambahan pula dengan menggunakan e-mel adalah tidak mudah identiti fizikal seseorang (sama ada jantina ataupun umur) dikenalpasti. Oleh itu pengenalan diri pelaku e-jenayah sentiasa "terlindung".

Maka terbuktilah di sini bahawa Internet mampu menyediakan satu alat komunikasi yang sangat berkesan dan boleh menjayakan perlakuan jenayah disempurnakan dengan licik (Parker, 1998).

4.2 Klasifikasi & Modus Operandi

Pada masa kini didapati ancaman jenayah komputer atau jenayah siber semakin mendesak. Ini memandangkan secara umumnya kehidupan keseluruhan masyarakat pada hari ini tidak dapat lari daripada menggunakan komputer. Menangani jenayah komputer dan jenayah siber memerlukan pemahaman yang menyeluruh mengenai kedudukan sebenar ancaman yang bakal diakibatkan olehnya (Wall, 2000). Definisi umum menjelaskan jenayah komputer sebagai meliputi perlakuan jenayah yang melibatkan aktiviti yang ada kaitan dengan komputer. Oleh itu amat wajar mengambil kira faktor

penggunaan komputer sebagai salah satu unsur utama dalam memperolehi keterangan (evidence), penyiasatan dan pendakwaan

Mengikut klasifikasi Biro Penyisatan Persekutuan (FBI), senarai jenayah komputer dan jenayah yang berkaitan dengan komputer yang telah disenaraikan oleh *National Computer Crime Squad* dan disiasat oleh pihak mereka adalah seperti berikut;

a. Pencerobohan ke atas rangkaian suis awam *(Public Switched Network)*
b. Menceroboh sistem rangkaian komputer
c. Pencabulan intergriti sistem rangkaian
d. Pencabulan persendirian *(Privacy Violation)*
e. Pengintipan industri *(Industrial Espionage)*
f. Perlanunan perisian komputer
g. Lain-lain– jenis jenayah yang menggunakan komputer sebagai alatan utama.

Berdasarkan pengertian yang diberikan oleh Organization for Economic Cooperation and Development (OECD) pula jenayah siber membawa maksud sebarang perlakuan yang bercanggah dengan undang-undang atau tingkahlaku yang membabitkan pemerosesan data secara otomatik atau transmisi data yang tidak dibenarkan. Oleh itu perlakuan berkenaan disifatkan sebagai jenayah mengikut tafsiran undang-undang, kerana ia melibatkan perlakuan yang tidak dibenarkan (unathorised behaviour).

Dalam hal ini ternyata teori dan kaedah 'tradisi' dalam pengendalian dan urusan mengesan atau mencegah jenayah menjadi amat sukar disebabkan sifat maya atau *'virtual'* yang terpaksa dihadapi oleh semua pihak untuk membolehkan penguatkuasaan undang-undang disempurnakan. Ini adalah disebabkan 'suasana-maya' yang wujud itu melewati batas sempadan geografi dan geo-politik sesebuah negara. Ini membolehkan seseorang penjenayah itu dengan mudah menjayakan sesuatu perlakuan jenayah di satu tempat yang lain (terutama sekali di tempat yang 'selamat' dari tindakan undang-undang) hingga melewati batas sempadan sesebuah negara itu dalam melancarkan gerakannya (Cheswick, 1994., Denning & Denning, 1997).

Ini merupakan salah satu cabaran yang perlu ditempuhi khususnya oleh pihak yang terbabit dengan penguatkuasaan undang-undang siber. Sungguhpun di sesetengah negara wujud perjanjian ekstradisi (yang mengizinkan penjenayah dipindahkan antara negara) dua hala tetapi bukannya mudah untuk disempurnakan, memandangkan perlakuan jenayah yang telah dilakukan mungkin tidak menjadi satu kesalahan pada negara berkenaan. Oleh itu dengan memiliki undang-undang atau peraturan yang berkaitan tidak bermakna sudah cukup untuk dikuatkuasakan kerana undang-undang berkenaan mungkin lebih bersifat lokal/tempatan dari segi jurisdiksinya (Roseneor, 1997).

Justeru, memiliki undang-undang yang dikira sofistikated dari segi kandungannya, bersifat pintar dan 'supra-national' tidak semestinya sudah lengkap dan mampu menangani masalah yang berbangkit dari kegiatan e-jenayah. Sebaliknya, ia perlu diperlengkapkan lagi dengan keupayaan yang benar-benar berkesan terutama sekali bagi mengatasi masalah yang berhubung dengan batas-sempadan dan batas kuasa perundangan sesebuah negara.

Perlakuan e-jenayah semakin meningkat dengan pesat dari sehari ke sehari dan menjadi lebih sofistikated dari sebelumnya. Laporan dari beberapa negara di dunia berkaitan dengan e-jenayah juga menunjukkan peningkatannya yang semakin serius. Mengikut Louis J. Freech[45], kadar jenayah komputer di Amerika Syarikat yang dilaporkan sebanyak 70% meliputi tindakan pencerobohan dan pencabulan sistem komputer milik organisasi dan individu. Di samping itu dalam laporan yang sama, ancaman *virus* dianggarkan sebanyak 85% dan salah-guna di kalangan pekerja sendiri (bagi sistem rangkaian milik syarikat) yang dikesan adalah sebanyak 79%. Antara perlakuan yang sering terdapat di kalangan penjenayah yang terbabit adalah 'mencuri' maklumat *proprietry*, penyelewengan kewangan, menceroboh masuk ke dalam sistem rangkaian, melancarkan serangan seperti *denial of service* dan tindakan sabotaj ke atas sistem maklumat atau data yang sedia ada. Daripada keseluruhan insiden seumpama ini, 24% mengakui bahawa tindakan yang sedemikian

[45] Pengarah *Biro Siasatan Persekutuan* Amerika Syarikat menyampaikan maklum-balas dari satu kaji-selidik terhadap 643 responden mengenai e-jenayah pada Mac 2000

mengakibatkan kerugian kewangan yang agak besar dengan anggaran US 120 juta. Peningkatan e-jenayah yang begitu banyak mendesak supaya langkah-langkah (khususnya berkaitan dengan undang-undang) yang berkesan disediakan terutama sekali untuk memastikan amalan ini dapat dihalang atau dicegah dengan cara yang paling efektif.

BAB 5

5. Komputer & Internet – Undang-undang & e-jenayah

Dari segi penguatkuasaan, undang-undang siber telah diperkenalkan melalui dua pendekatan umum, iaitu dari segi undang-undang dan sosio-ekonomi.

Dari segi undang-undang, matlamat utamanya ialah;

a. menyediakan keperluan untuk menghadapi kasalahan jenayah yang berkaitan dengan komputer

b. bertindak sebagai pelengkap kepada undang-undang jenayah yang sedia ada.

Dari segi sosio-ekonomi pula;

a. untuk menggalakkan usaha-usaha intelektual dalam bidang berkaitan dengan ICT
b. menyediakan suasana yang sesuai dengan industri multimedia dan juga bertujuan untuk memajukan kegiatan perdagangan elektronik

Pelaksanaan undang-undang siber di Malaysia disifatkan sebagai usaha untuk memenuhi sebahagian dari kerangka komprehensif dari perspektif undang-undang. Di samping untuk memenuhi kehendak masyarakat semasa dan keperluan kegiatan perdagangan elektronik yang semakin berkembang dengan pesat (sama ada untuk tujuan pemasaran produk, perkhidmatan atau maklumat). Pada masa yang sama penyediaan peruntukan undang-undang yang bersesuaian akan dapat memberi perlindungan yang berpadanan bagi berbagai kegiatan, khususnya yang berkaitan dengan harta-intelek (intellectual

property), tandatangan digital, jenayah komputer, pengajian jarak jauh (dalam talian) – *online distance learning - telemedicine,* kerajaan elektronik dan lain-lain.

Lantaran itu undang-undang siber memainkan peranan amat penting untuk mempastikan perlidungan keselamatan kepada sistem maklumat, intergriti sistem rangkaian komputer dan kebolehpercayaan sentiasa dapat dikekalkan. Hasilnya pembangunan komunikasi dan pertumbuhan industri multimedia akan lebih terjamin dan mampu meletakkan Malaysia sebagai hub utama di rantau ini dalam bidang komunikasi dan multimedia.

Sememangnya ramai bertanggapan undang-undang konvensional yang sedia ada tidak mampu menghadapi e-jenayah yang telah sedia sofistikated disebabkan jenayah hari ini mempunyai kaitan langsung dengan penggunaan komputer. Oleh itu, amat penting disediakan undang-undang khusus menghadapi jenayah siber atau jenayah komputer. Sungguhpun sesetengah jenayah itu bersifat konvensional tetapi disebabkan adanya kemajuan teknologi komputer hari ini telah menyebabkan banyak kegiatan e-jenayah menjadi semakin kompleks dan sukar dikesan apatah lagi untuk dihadapkan ke mahkamah.

Berdasarkan laporan yang dikeluarkan oleh *International Intellectual Property Alliance* (IIPA), semenjak mereka melancarkan kegiatan merampas produk harta intelek yang dicetakrompak pada Mac 2001 tiada satu pun

tindakan susulan diambil untuk membawa pelaku e-jenayah yang terbabit ke mahkamah[46]. Dalam laporan yang sama juga ada menyebut bahawa dianggarkan sebanyak 2.8 billion hasil karya muzik, filem dan fail dalam format digital dimuat-turunkan (downloaded) setiap bulan melalui Internet di seluruh dunia. Ini membuktikan tanpa kekuatan akta atau undang-undang yang kukuh dan berkeupayaan usaha-usaha mendakwa pelaku e-jenayah menjadi tidak berkesan. Akibatnya, langkah untuk membatasi apatah lagi untuk menghalang kegiatan mereka yang kini semakin berleluasa tidak akan berjaya. Justeru akan menjejaskan usaha-usaha membangunkan kegiatan perdagangan dan perniagaan khususnya dalam industri muzik dan perfileman kerana sektor industrilah yang paling teruk menerima akibatnya.

Di samping melindungi golongan pemodal dan peniaga, undang-undang siber juga berperanan menyediakan perlindungan yang bersesuaian kepada para pengguna, terutama untuk melindungi hak mereka terutama sekali apabila transaksi elektronik dijalankan. Dengan cara itu, golongan peniaga akan dilindungi dengan kerangka-kerja yang jelas dari segi perundangannya terutama sekali dalam menyediakan platform urusniaga secara digital atau elektronik tanpa sebarang konflik yang mungkin boleh berbangkit kemudiannya. Manakala pengguna pula akan turut menerima perlindungan

[46] Dipetik dari laporan akhbar The Star, 9hb Mac 2002 – *In.Tech* ms. 4

yang serupa sebagaimana perlindungan yang diberikan dalam amalan perdagangan konvensional.

Namun begitu, sehingga setakat ini pihak kerajaan berupaya menghalang dan mengawal kegiatan e-jenayah yang bersifat *'virtual'* yang berlaku di ruang siber khususnya untuk membolehkan kepentingan orangramai sentiasa dilindungi dari ancaman jenayah siber. Tindakan ini sejajar dengan kehendak dan keperluan ketetapan resolusi Bangsa-bangsa Bersatu yang diputuskan dalam satu sidang Perhimpunan Agung PBB yang dikenali sebagai *Combating the Criminal Misuse of Information Technologies*[47].

5.1 Memahami e-jenayah

Salah satu undang-undang siber yang paling awal diperkenalkan dan menjadi teras utama dalam menangani e-jenayah di Malaysia ialah Akta Jenayah Komputer 1997 (Computer Crime Act 1997), yang pada sifatnya menjelaskan matlamat untuk memerangi jenayah aktiviti komputer, jenayah siber dan jenayah yang berkaitan dengan komputer yang semua terangkum sebagai e-jenayah.

Berdasarkan pengertian yang diberikan dalam seksyen 2, komputer didefinisikan sebagai peralatan yang berkeupayaan untuk memproses data, iaitu

[47] *"Assembly Condemns Misuse of Information Technologies for Criminal Purposes"* United Nation GA/9842 – 4th December 2000.

antaranya ialah *router, computer switches*, dan juga peralatan *micro-processor* yang terdapat pada peralatan seperti mesin-basuh dan kamera.

Walau bagaimanpun, jika diteliti Akta ini tidak pula menjelaskan secara khusus pengertian 'jenayah siber'. Namun begitu, pengertian yang diberikan dalam seksyen 2 dianggap sudah cukup jelas untuk menerangkan semua kegiatan jenayah yang dilakukan dalam lingkungan rangkaian sistem jaringan komputer sebagai jenayah komputer atau jenayah siber. Begitu juga kegiatan atau amalan jenayah yang dilakukan dalam jaringan rangkaian komunikasi dan komputer yang dihubungkan turut termaktub dalam Akta ini.

Ringkasnya mengikut pengertian Akta ini terdapat dua jenis jenayah komputer, iaitu pertama yang berkaitan dengan *data interception, data interpretation*, mencuri data, mengganggu-gugat rangkaian (network interference), sabotaj sistem rangkaian, menceroboh sistem rangkaian, memecah-masuk tanpa kebenaran, menyebar virus atau cecacing, *spamming, mail-bombing*, menyebar kod-jahat, *identity theft*, dan tindakan menggodam sistem rangkaian.

Jenis jenayah yang kedua lebih tertumpu kepada perlakuan jenayah yang berkaitan dengan penggunaan komputer, yakni perlakuan jenayah konvensional tetapi menggunakan komputer sebagai alatan utama. Ini meliputi perlakuan jenayah seperti yang ditakrifkan dalam Kanun Kesiksaan.

Antara perlakuan yang ditakrifkan oleh Kanun Kesiksaan (Akta 574) termasuk menipu, *criminal intimidation*, menghina atau mengganggu, kesalahan berkaitan perkahwinan, *defamation*, pemalsuan, kesalahan yang berkaitan dengan timbang dan ukuran dan melakukan penjualan produk terlarang.

5.2 Jenis-jenis e-jenayah: tafsiran undang-undang

Antara kesalahan e-jenayah yang ditakrifkan oleh Akta ini misalnya dalam seksyen 3 antara lain ialah tindakan yang bertujuan memperolehi maklumat tanpa kebenaran. Akta ini menjelaskan kesalahan e-jenayah jenis ini dilakukan melalui tindakan hingga menyebabkan komputer melakukan fungsi yang membenarkan perlakuan untuk mengakses masuk tanpa kebenaran pemiliknya tetapi tidak semestinya ditujukan kepada sesuatu data atau program perisian tertentu.

Manakala seksyen 4, ditujukan kepada kesalahan jenayah yang melibatkan tindakan mengakses tanpa kebenaran dengan tujuan untuk melakukan atau melaksanakan perlakuan jenayah yang melibatkan penipuan atau kecederaan tanpa mengambil kira sama ada perlakuan itu dilakukan pada masa yang sama atau masa yang akan datang.

Seksyen 5, menyentuh tentang tindakan melakukan modifikasi kandungan data atau sistem maklumat sedia ada tanpa kebenaran sama ada bersifat sementara atau kekal. Seksyen 6 pula menyebut adalah menjadi satu

jenayah kepada mana-mana pihak yang bertindak memaklumkan sesuatu nombor, kod, kata laluan atau sesuatu yang membolehkan seseorang yang lain mengakses sesuatu sistem maklumat tanpa kebenaran.

Bagi tujuan penyiasatan pula, seksyen 10 menjelaskan pihak magistret berhak mengeluarkan waran untuk menggelidah di premis tertuduh dan juga di premis tempat mangsa dengan tujuan menghimpun maklumat atau keterangan. Di bawah seksyen yang sama di perenggan ke 2 menghendaki orang yang disyaki membantu pihak berkuasa memperolehi maklumat seperti mana yang dikehendaki mereka. Sekiranya permintaan pihak berkuasa tidak dipenuhi oleh orang yang disyaki, mereka boleh dikenakan tindakan sama seperti cuba menghalang pihak berkuasa daripada menjalankan kewajipan yaang adalah menjadi satu kesalahan di bawah seksyen 11.

Terdapat empat kategori utama yang ditakrifkan oleh Akta Jenayah Komputer (1997) iaitu;

i. *Perlakuan jenayah atau tindakan yang disasarkan ke atas komputer atau rangkaian komputer atau peralatan komputer* – meliputi tindakan mencuri atau merosakkan komputer, atau pada peralatan komputer yang dapat dilihat secara nyata seperti dilakukan ke atas cekera-keras, disket, cekera padat dan cakera optik yang mengandungi data atau program atau perisian ataupun ke atas peralatan komputer yang lainnya. Biasanya jika kesalahan seumpama ini

dilakukan, peralatan atau perkakasan komputer dapat dikemukakan sebagai bahan bukti untuk mendakwa pihak yang melakukan perbuatan berkenaan. Dalam keadaan ini ia tidak memerlukan khidmat tenaga pakar dalam memperolehi maklumat yang diperlukan (NIJ, 2000).

Namun begitu, terdapat keadaan apabila kerosakan berlaku akibat tindakan e-jenayah, tetapi tidak dapat dilihat secara nyata (fizikal) dan kadangkala sukar dikesan apatah lagi untuk menilainya secara kuantitatif. Situasi ini boleh berlaku dalam keadaan apabila data atau maklumat telah dibaca atau disalin tanpa kebenaran, mungkin juga dipinda atau dipadam langsung ataupun tindakan dengan sengaja meminda hingga boleh mengakibatkan program atau perisian berkenaan terjejas atau tidak berfungsi lagi (Wolff, 1996). Tindakan sedemikian rupa biasanya tidak meninggalkan kesan fizikal yang nyata dan sukar untuk dibuktikan dengan mudah.

Selain dari itu terdapat juga tindakan e-jenayah yang ditujukan ke atas komputer atau sistem rangkaian dengan menggunakan virus atau cecacing yang disebarkan dengan sengaja sama ada dengan menggunakan disket atau media pengstoran tertentu atau melalui Internet seperti menggunakan e-mel yang dihantar kepada seseorang atau kepada pelayan e-mel. Kadangkala dilakukan secara bertubi-tubi hingga boleh melumpuhkan sistem rangkaian komputer yang menjadi sasaran (Pipkin, 1997). Satu lagi kaedah yang seumpama ini dengan melancarkan serangan melalui e-mel yang diinfeksi dengan virus atau

cecacing (Cohen, 1994), ialah dengan menggunakan kaedah *Trojan-horse*, dilakukan dengan meletakkan *trojan* berkenaan didalam sesuatu sistem komputer atau dalam rangkaian komputer dan kemudiannya dibiarkan bertindak mengikut masa yang telah ditetapkan.

Penyiasatan bagi insiden yang dikemukakan di atas memerlukan bantuan dan sokongan khidmat pakar 'forensik komputer' untuk mengesan bukti-bukti yang boleh diperolehi. Selalunya penyiasatan yang dilakukan oleh pakar yang berkaitan berlandaskan keterangan sokongan – *circumstantial evidence* – memandangkan amat sukar untuk mendapatkan saksi-langsung bagi membuktikan kesalahan berkenaan.

Walau bagaimanapun dengan menggunakan sistem keselamatan yang baik, kemungkinan untuk mengesan semula bukti-bukti yang menunjukkan kesalahan atau boleh disabitkan kesalahan yang telah dilakukan mungkin akan dapat dilaksanakan. Kaedah pengesanan dapat dilakukan dengan melihat semula rekod seperti '*time-stamp*', *Internet Protocol Address*, *Manufacturer Acess Code* (MAC). Oleh itu amat wajar sekali untuk memiliki tenaga pakar dalam bidang berkaitan bagi tujuan menghimpun maklumat yang diperlukan. Terutama sekali bagi menjelaskan perkara-perkara yang berkaitan dengan isu-isu teknikal yang kompleks yang biasanya wujud dalam sesuatu sistem komputer (NWCCC, 2001). Dalam keadaan tertentu, siasatan yang dilakukan adalah perlu untuk

membuktikan bahawa sistem komputer yang disiasat itu 'boleh-dipercayai' dan semua kata-laluan dan ID digunakan mengikut prosedur yang telah ditetapkan.

ii. Kesalahan yang dilakukan dengan menggunakan komputer, atau rangkaian komputer – Pada umumnya hampir semua pakar komputer sependapat bahawa dengan menggunakan komputer sebagai alat tidak menjadikan kesalahan mereka dengan sebagai "jenayah komputer". Sebaliknya klasifikasi sesuatu jenayah itu seharusnya dilihat dari akibat perlakuan kesalahan jenayah yang dilakukan dan bukan akibat alat yang digunakan. Oleh itu tidak wajar disifatkan sebagai jenayah komputer atau jenayah siber semata-mata kerana menyebarkan "khabar angin" melalui Internet.

Terdapat juga yang menghujah bahawa perlakuan berkenaan boleh disifatkan sebagai jenayah siber kerana tindakan menggunakan e-mel dan Internet telah membolehkan penyebaran maklumat yang begitu cepat dan meluas. Kesan yang menyeluruh dari keadaan tersebut tidak mungkin akan berlaku jika hanya menggunakan keadah penghantaran surat konvensional yang bukan sahaja lambat tetapi tidak mungkin tersebar meluas dalam jangkamasa yang singkat. Oleh itu penggunaan alat komputer dan rangkaian komputer yang sedia ada berjaya menyebarkan maklumat dengan sebegitu cepat dan meluas. Seharusnya ia disifatkan juga sebagai jenayah siber.

Begitu juga dengan perlakuan jenayah seperti memperolehi maklumat rahsia, meminda urusniaga yang dilakukan secara *online*, memperolehi maklumat sulit yang lain seperti nombor akaun, ID pengguna, kata-laluan, atau nombor kad kredit (untuk tujuan pemalsuan atau mengklon kad kredit) untuk tujuan penipuan. Di samping itu juga sesetengah maklumat mungkin digunakan bagi tujuan memeras-ugut seseorang.

Usaha mengendalikan penyiasatan e-jenayah, amat memerlukan khidmat pakar yang mampu memberi maklumat penting, terutama sekali membuktikan bahawa kemudahan komputer atau rangkaian komputer sentiasa tersedia kepada pihak tertuduh tanpa sebarang halangan. Pada masa yang sama kemudahan yang sedia ada itu sentiasa berfungsi dengan baik bagi membolehkan kegiatan e-jenayah dapat disempurnakan oleh pihak tertuduh. Di samping itu ia juga bergantung kepada sesuatu keadaan kes sama ada pihak penyiasat memerlukan keterangan dari pentadbir-sistem rangkaian komputer – *system administration* – atau keterangan pakar (seperti yang diperuntukkan oleh sekyen 45, Akta Keterangan, 1954).

Selain dari itu, amat penting untuk membuktikan juga segala peralatan yang berkaitan bagi melakukan kesalahan yang dimaksudkan benar-benar berfungsi sama ada dari segi perkakasan ataupun perisian. Misalnya sistem komputer yang digunakan memiliki keupayaan seperti mana yang sepatutnya, misalnya

tertuduh disyaki melakukan tindakan muat-turun (download) maklumat atau data melalui cara mengakses tanpa kebenaran.

Bagi insiden yang melibatkan perlakuan mencuri data atau maklumat sulit, selalunya disempurnakan dengan menggunakan program atau perisian *sniffer* yang biasanya 'ditanam' di dalam komputer atau rangkaian komputer yang disasarkan atau menggunakan perkakasan khusus untuk maksud yang sama. Keadaan seumpama ini amat perlu sekali dibuktikan bahawa perisian/progam atau alat yang dimaksudkan bukan setakat tersedia ada bagi kegunaan orang yang disyakki tetapi juga terbukti berkemampuan untuk melakukannya seperti mana yang dikehendaki. Selain dari itu, untuk tujuan pendakwaan pula amat perlu dibuktikan bahawa yang tertuduh bertanggungjawab 'menanam' alat berkenaan dan mempunyai niat (*mens rea*) untuk melakukan jenayah dengan menggunakan alat berkenaan bagi tujuan mencuri maklumat rahsia yang diperlukan.

iii. Kesalahan ke atas harta intelek. Kebanyakan kesalahan jenis ini melibatkan tindakan yang dilakukan oleh pesalah e-jenayah melalui tindakan 'melanun' atau cetak rompak hasil karya intelektual seperti genre muzik dan filem di samping juga perisian atau program komputer. Walaupun pada umumnya hasil karya muzik, filem, perisian komputer dan lain-lainnya terlindung di bawah Akta Hak Cipta 1987, tetapi dalam hal yang sebenar industri ini menjadi

mangsa utama. Sungguhpun berbagai usaha[48] dilakukan bagi memerangi e-jenayah ini termasuk merampas cakera padat cetak rompak yang dijual seperti yang dilakukan oleh IIAP tetapi sehingga kini belum menampakkan sebarang hasil. Dari tindakan merampas dilakukan kira-kira setahun yang lalu tiada suatu pun yang berjaya dibawa ke muka pengadilan (jenayah – sebaliknya kebanyakan tindakan yang dilakukan dengan mengemukakan tuntutan saman sivil yang didapati lebih mudah untuk memenangi kes yang berkaitan).

iv. Kesalahan yang disifatkan sebagai hasil penggunaan komputer atau rangkaian komputer secara tidak bertanggungjawab. Bagi kategori kesalahan yang berkaitan salahlaku, di bawah seksyen 6, Akta Jenayah Komputer (1997) menetapkan bahawa setiap pengguna komputer atau komputer rangkaian seharusnya bertanggungjawab dan patuh serta akur dengan aturan yang telah ditetapkan. Adalah menjadi kesalahan di bawah seksyen ini untuk menyampaikan sama ada secara langsung atau tidak langsung mengenai sebarang maklumat seperti kod, nombor, kata-laluan atau lain-lain maklumat yang boleh digunakan bagi tujuan mengakses sesuatu sistem komputer. Segala maklumat sulit seharusnya sentiasa terpelihara dari sebarang ancaman dari didedahkan dengan sengaja. Oleh itu cadangan untuk mewujudkan Undang-undang Perlindungan Data

[48] Antara peraturan yang ditetapkan termasuk mewajibkan semua pengeluar cakera padat mencetak nombor siri pengeluaran bagi setiap cakera padat yang dihasilkan dari kilang mereka. Dengan cara itu lebih mudah mengesan cakera padat cetak rompak dihasilkan dari dari pengeluar mana

amat dialu-alukan supaya segala maklumat sulit, peribadi atau maklumat awam sentiasa dilindungi oleh undang-undang.

5.3 Menjejaki e-jenayah

Dalam usaha untuk menjejaki e-jenayah perkara yang amat penting perlu diingat terutama sekali untuk memperolehi maklumat atau keterangan yang mampu digunakan untuk tujuan pendakwaan. Oleh itu, segala maklumat berhubung dengan kegiatan e-jenayah (sebahagian besar maklumat utama adalah dalam bentuk data elektronik yang dihasilkan dari komputer dan sistem rangkaian komunikasi yang bersifat "mudah dimusnahkan") mestilah diperolehi. Keterangan elektronik adalah merupakan maklumat dan data yang amat berharga dan yang digunakan untuk tujuan siasatan. Kebanyakan maklumat ini tersimpan dalam perkakasan khusus seperti media pengstoran elektronik dan proses siarrayanya hanya dapat dilakukan dengan menggunakan peralatan elektronik.

Pada umumnya sifat data elektronik tidak dapat dilihat secara fizikal walaupun sebahagiannya boleh dicetak atau dipaparkan di skrin. Sungguhpun begitu kebanyakan pakar forensik komputer sependapat bahawa maklumat data digital ini adalah seumpama DNA – *deoxyribonucleic acid* – yang memiliki sifatnya tersendiri. Oleh itu, data digital boleh didedahkan hanya melalui teknik atau kaedah khusus dengan menggunakan peralatan elektronik dan

perisian yang khusus untuk memperolehi maklumat berkenaan. Justeru amat perlu diperolehi testimoni yang dapat memberi penerangan bagi memeriksa maklumat yang diperlukan dan juga untuk menjelaskan mengenai kandungan maklumat elektronik.

Walau bagaimanapun keadaan ini akan menjadi lebih rumit apabila perlakuan jenayah yang telah dilakukan itu berlaku melalui penggunaan rangkaian Internet. Ini adalah kerana 'laluan' Internet yang sentiasa disertai jutaan pengguna daripada seluruh pelosok dunia akan mengakibatkan kemungkinan maklumat berkenaan 'terhapus' dan tidak mungkin diperolehi semula. Lantaran itu, keterangan yang ingin diperlukan oleh pihak pendakwa akan lebih sulit dan mencabar. Pada umumnya, untuk memperolehi sebarangan maklumat atau keterangan sama ada bagi tujuan siasatan atau pendakwaan adalah sangat rumit. Kerumitan ini bertambah lagi apabila urusan mendapatkan maklumat hanya boleh dilakukan dengan menggunakan perkakasan khas.

Oleh yang demikian langkah-langkah waspada perlu diambil bagi mempastikan keterangan atau maklumat yang diperlukan bagi tujuan pendakwaan tidak dikompromi. Jika tidak boleh menimbulkan halangan besar kepada pihak pendakwa dan mengakibatkan usaha pendakwaan penjenayah elektronik di mahkamah akan terjejas begitu sahaja.

Usaha untuk menghimpun maklumat yang diperlukan melibatkan proses mencari, mengenalpasti, mengumpul dan mendokumen segala maklumat elektronik yang diperlukan bagi tujuan menyediakan segala keterangan yang diperlukan bagi mendakwa tertuduh. Proses menghimpun boleh dilakukan sama ada secara masa nyata – *real-time* – atau diperolehi dari maklumat yang terkandung dalam sistem pengstoran yang terdapat pada sesuatu komputer. Sewaktu menghimpun segala maklumat ini, adalah penting bagi seseorang untuk sentiasa ingat supaya berhati-hati agar tiada data yang cuba diperolehi itu akan terpinda, termusnah atau hilang begitu sahaja. Sekiranya ini berlaku bukan sahaja lebih sukar untuk menjayakan usaha-usaha menghimpun data, malahan boleh menggagalkan tindakan pendakwaan di mahkamah nanti[49].

Peringkat kedua melibatkan peringkat pemeriksaan. Beberapa langkah awal perlu diambil bagi mempastikan supaya usaha untuk mengenal pasti maklumat dapat disempurnakan dengan baik, terutama sekali untuk mengenalpasti asal sumber data, kesignifikanan maklumat yang telah dihimpunkan dan membolehkan maklumat atau keterangan itu dikemukakan secara *visible*. Langkah awal yang perlu dilaksanakan ialah mendokumenkan segala kandungan dan keadaan – *state* – maklumat atau keterangan secara menyeluruh. Dengan mendokumentasikan secara ini, semua pihak yang

[49] U.S. Department of Justice (2001) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Washington D.C.

terbabit dapat melihat kandungan data elektronik yang terdapat di dalamnya. Hanya dengan mengambil langkah berkenaan maka barulah segala maklumat yang terlindung atau sengaja disorokkan atau yang dikriptografikan dapat dikenalpasti dan boleh digunakan untuk tujuan pendakwaan.

Untuk membolehkan penyiasatan e-jenayah dijalankan bagi kesalahan menghantar virus melalui Internet, amat perlu penyiasatan dilaksanakan dengan mengemukakan keterangan *circumstantial* untuk membuktikan perlakuan yang telah dilakukan oleh tertuduh. Secara hipotetikalnya sesuatu penyiasatan itu perlu dibuktikan dengan mengemukakan keterangan berikut:

a) wujudnya virus di komputer milik tertuduh

b) terdapatnya rekod masa tertuduh melayari Internet.

c) maklumat direkodkan dalam log fail yang menunjukkan tertuduh mengakses komputer miliknya dan milik penerima pada waktu virus berkenaan dihantar.

d) terdapat bukti yang menunjukkan *auto-run* program telah ditetapkan mengikut masa yang khusus.

e) terdapatnya bukti-bukti jejak digital yang boleh dikemukakan sebagai maklumat seperti time-stamp, alamat TCP/IP milik tertuduh dan penerima (virus) di samping kod akses pengeluar (MAC)

f) terdapat juga bukti maklumat ID login yang boleh diperolehi dari ISP (maklumat ini akan mengesahkan tertuduh adalah orang yang bertanggungjawab menghantar virus)

Berdasarkan situasi di atas, penyiasatan yang dijalankan mampu mendedahkan kebenaran apabila pegawai penyiasat berjaya mengesan dan

mengenalpasti program virus yang tersimpan di dalam komputer milik tertuduh. Ditambah pula tarikh dan masa virus berkenaan dihasilkan atau dimodifikasikan boleh diperolehi dengan cara merujuk kepada *time-stamp*. Seterusnya bukti yang mesti dikemukakan ialah komputer milik tertuduh sentiasa berada di dalam keadaan yang baik dan boleh digunakan. Tertuduh juga sentiasa mempunyai kawalan langsung ke atas penggunaannya dan memiliki kemudahan Internet.

Corroborative evidence sungguhpun tidak diperlukan tetapi mampu untuk membuktikan tahap kemampuan dan keupayaan tertuduh dalam penggunaan komputer. Keterangan ini diperkukuhkan apabila didapati wujud perisian *assembly language* seperti jenis *C-programming* atau yang seumpamanya terdapat di dalam komputer milik tertuduh. Di samping itu terdapat bukti yang tertuduh juga telah menggunakan program berkenaan untuk menghasilkan pengaturcaraan virus atau cecaing. Sungguhpun begitu, maklumat ini tidak semestinya mempunyai pertalian langsung untuk menjelaskan perlakuan jenayahnya. Pihak penyiasat juga perlu memperolehi maklumat yang lain, terutama sekali adakah tertuduh memiliki program virus yang dimaksudkan dan bukti berkenaan merupakan bukti yang mungkin boleh mengheretnya ke mahkamah.

Namun begitu, untuk memperolehi keterangan seumpama di atas merupakan satu cabaran yang besar memandangkan sistem komputer yang ada

hari ini mempunyai keupayaan yang tinggi dan kompleks. Justeru itu, apabila sesuatu komputer "dirampas" amat perlu mempastikan semua data dan program perisian serta dokumen yang terkandung di dalam cakera keras mestilah disalin sepenuhnya (mirror copying). Sebaiknya dengan menggunakan CD-R untuk mempastikan kesemua maklumat diperolehi disalin dan pada masa yang sama untuk membolehkan pengesahan yang tidak boleh dipertikaikan (Casey, 2000). Walau bagaimanapun dalam sesetengah keadaan pihak penyiasat terpaksa berdepan dengan maklumat yang dikategorikan sebagai *privilege information.*

Dalam proses merampas bahan bukti jenayah ianya haruslah dilakukan dengan mengambil langkah-langkah atau prosedur tertentu bagi mempastikan kandungan maklumat di dalam cakera keras atau komputer tidak 'terpinda' atau 'termusnah'. Ini kerana dalam sesetengah komputer telah sedia terdapat perisian yang bertujuan memadam dokumen-dokumen atau maklumat apabila intigriti komputer berkenaan dikompromi oleh pengguna yang tidak dibenarkan (termasuk pegawai penguatkuasa yang cuba untuk menghimpun maklumat yang terkandung di dalamnya). Oleh yang demikian, amat perlu diambil langkah berjaga-jaga supaya maklumat atau keterangan yang terkandung di dalam komputer berkenaan tidak mudah "termusnah" sewaktu usaha-usaha ini dijalankan. Sungguhpun begitu, pada masa kini sudah terdapat perisian khusus yang mempunyai peranan untuk membolehkan maklumat atau

rekod elektronik yang dipadamkan atau dimusnahkan diperolehi semula (Denning, 1999). Pihak penyiasat juga perlu sentiasa berwaspada dan berkeupayaan menyempurnakan tugas untuk menghimpun, mendokumentasi, mengekal dan mengesahkan kesahihan keterangan elektronik yang terkandung di dalamnya.

Di samping itu, amat perlu mengambil langkah-langkah kawalan supaya komputer berkenaan tidak terdedah kepada unsur-unsur luaran yang lain seperti kepanasan (heat), medan magnet dan bahan beradiasi. Oleh itu amat penting kesemua langkah untuk memperolehi keterangan disempurnakan agar ianya dapat digunakan untuk tujuan pendakwaan di mahkamah. Salah satu langkah yang terpenting untuk memperolehi maklumat atau keterangan yang berkaitan dengan jenayah komputer ialah sebaik sahaja sesuatu perlakuan itu dikesan, prosedur atau protokol yang telah ditetapkan dilaksanakan secepat mungkin.

Dalam hal ini, pencontoh (template) penyiasatan bukan sahaja mesti bersifat luwes tetapi juga disepadukan kerana pengalaman telah membuktikan setiap satu jenayah yang berkaitan komputer adalah unik dan perlu dikendalikan mengikut kaedah-kaedah yang khusus dan dinilaikan mengikut kes yang disiasat. Pada kebiasaannya cetakan dokumen yang diperolehi sudah mencukupi dan memadai asalkan cetakan berkenaan memenuhi syarat yang ditetapkan di bawah seksyen 90 Akta Keterangan (1950), iaitu dokumen yang

dihasilkan oleh sesuatu komputer mestilah berada dalam keadaan perlu baik dari segi penggunaan biasa. Bagi tujuan ini juga, satu sijil yang ditandatangani (seperti yang telah ditetapkan di bawah sub seksyen 90(A)(3)(a) akta yang sama) oleh orang yang berkenaan, yang semestinya bertanggungjawab dalam pengurusan dan penghasilan dokumen yang dihasilkan oleh komputer. Sijil ini mestilah disertakan dengan dokumen yang akan dikemukakan di mahkamah. Kandungan sijil yang dikemukakan itu mestilah menyatakan bahawa maklumat yang terkandung di dalam dokumen adalah sah seperti mana dalam operasi sesuatu dokumen.

5.4 Menangani e-jenayah

Di Malaysia insiden seumpama ini juga sering dilaporkan kepada berbagai pihak yang berkaitan. Mengikut rekod laporan e-jenayah yang dilaporkan oleh Bernama[50] sebanyak 2,503 kes yang dikesan. Kegiatan ini telah berlaku antara 1997 sehingga Jun 2001 yang membabitkan berbagai bentuk atau jenis e-jenayah. Antaranya insiden yang dilaporkan ialah pencerobohan sistem rangkaian komputer, penyebaran virus, *mail-bomb*, dan perlakuan lain yang berkaitan[51].

Untuk menghadapi ancaman yang berkaitan dengan e-jenayah, Malaysia telah pun memulakan usaha-usaha awalnya. Ini memandangkan dasar negara

[50] Laporan BERNAMA pada 9hb Ogos 2001

[51] Angka yang diberikan ini tidak termasuk insiden yang berpunca dari *Code-Red-Worm*, mengikut laporan sebanyak 1,930 rangkaian sistem komputer yang menerima padah serangan cecacing jenis ini.

yang ingin menggerakkan dan memesatkan pertumbuhan negara berlandaskan kepada teknologi maklumat dan komunikasi (ICT) maka amat wajar diberi perlindungan dari ancaman e-jenayah. Jika tidak pertumbuhan ekonomi berasaskan kepada ICT akan terjejas. Dianggarkan bahawa pada tahun 2002 pelaburan dan perbelanjaan dalam sektor industri ICT di Malaysia adalah bernilai RM 9.12 billion berbanding RM 8.36 billion pada tahun 2001[52].

Pada tahun 1996, Agenda Kebangsaan Teknologi Maklumat (NITA – National IT Agenda) telah ditubuhkan yang merupakan sebahagian daripada strategi utama yang disasarkan dalam pelan jangka masa panjang pembangunan negara. Usaha ini sejajar dengan usaha persediaan untuk menyahut cabaran era teknologi maklumat yang sedang berkembang pesat pada masa itu. Agenda berkenaan mengandungi garis panduan kasar bagi kerangka kebangsaan yang bermatlamat menyediakan pembangunan ICT yang seimbang untuk masyarakat dan negara Malaysia[53]. Matlamat ini akan hanya dapat dicapai sekiranya masyarakat dan negara mampu memberi sepenuh kepercayaan terhadap pertumbuhan teknologi maklumat, yang ternyata akan hanya dapat dicapai melalui sistem keselamatan ICT yang mantap.

---

[52] NST, Computimes 25 April 2002.

[53] Ucapan Dato' Seri Dr. Mahathir sewaktu mengisytiharkan Perlantikan Panel Baru dalam NITA 23 April 2002

Pada bulan Mac 1997, *Malaysian Computer Emergency Response Team* (MyCERT) telah dilancarkan. Peranan utama *MyCERT*[54] adalah untuk menyediakan platform bagi memberi bantuan kepada semua pengguna ICT dari segi keselamatan dan ancaman berkaitan dengan pencerobohan, *denial of service*, ancaman penggodam, serangan kod-jahat (malicious code attack), salahguna e-mel dan lain-lain yang berkaitan. Serentak dengan pertumbuhan yang semakin pesat dalam penggunaan ICT dan tuntutan yang meningkat dalam usaha mengatasi ancaman e-jenayah, didapati timbul keperluan yang lebih mendesak supaya satu badan induk yang lebih berkaliber diwujudkan.

Ini memandangkan pertumbuhan teknologi ICT yang lebih pesat mengkehendaki supaya satu platform yang lebih mantap dan utuh disediakan untuk menangani ancaman yang boleh berlaku ke atas prasarana ICT yang sedia ada, di samping untuk memenuhi kehendak pengguna ICT sama ada individu atau organisasi. Maka pusat rujukan ICT yang lebih berwibawa dan mengkhususkan peranan mereka dalam menangani isu-isu keselamatan ICT secara proaktif amat diperlukan. Lebih-lebih lagi apabila berbagai aplikasi dan peralatan atau perkakasan komputer yang dihasilkan oleh pengeluar pada masa kini didapati kurang menitikberatkan keperluan keselamatan berbanding dengan keperluan penggunaannya (funtionality).

---

[54] Sila rujuk www.mycert.org.my

Atas desakan yang seumpama ini dalam Mesyuarat Majlis Teknologi Maklumat Kebangsaan (National Information Technology Council) ke 6 pada 15hb Januari 1998, telah membuat keputusan untuk menubuhkan Pusat Respon Kecemasan dan Keselamatan ICT Kebangsaan (NISER – National ICT Security and Emergency Response Centre) dengan matlamat menangani persoalan utama berhubung isu keselamatan ICT yang bakal dihadapi oleh negara. Dengan kehadiran NISER, agensi ini mampu menjalankan berbagai langkah dan aktiviti termasuk mewujudkan hubungan kerjasama dengan berbagai agensi (kerajaan dan organisasi swasta) yang lain bagi menghadapi pelbagai perkara yang berkaitan dengan keselamatan ICT. Antara visi dan tanggungjawab penting yang dimainkan oleh NISER ialah;

a. Mengekalkan dan mempertingkatkan tahap kompetensi teknikal;
b. Menyediakan pelan tindakan proaktif bagi menghadapi ancaman dan keperluan keselamatan ICT;
c. Mengukuhkan tahap kerjasama dengan semua pihak tanpa mengambil kira batas sempadan geografi atau politik dan berterusan meneraju evolusi perkembangan keselamatan ICT negara;
d. Mengekalkan sebagai agensi yang bersifat neutral dan tidak memihak dalam berbagai usaha dan tindakan misalnya berkongsi maklumat yang relevan, metodologi tindakan yang transparent dan berkomunikasi secara terbuka;
e. Sebagai agensi yang tidak bermatlamatkan keuntungan.

Berlandaskan visi dan peranan NISER, agensi ini telah menjalankan berbagai aktiviti termasuk menyediakan laman-webnya iaitu www.niser.org.my. Salah satu usaha awal NISER ialah menjalankan satu kajiselidik sepanjang

bulan Jun 2001[55] untuk memperolehi maklumat yang berkaitan dengan insiden e-jenayah di kalangan organisasi awam dan swasta.

Hasil kajiselidik yang dijalankan itu didapati kebanyakan organisasi (awam dan swasta) di Malaysia iaitu 68% dari 205 organisasi yang telah disurvei mengalami tahap ancaman insiden pencerobohan yang tinggi terhadap rangkaian sistem komputer atau sistem maklumat milik mereka. Antara bentuk ancaman yang sering dihadapi adalah terdiri dari serangan virus[56] sehingga mengakibatkan kerugian yang dianggarkan sehingga RM 239,000.00 berdasarkan kepada maklumat dari oleh 113 organisasi[57] yang telah ditemubual. Di samping itu laporan survei berkenaan telah menunjukkan insiden kecurian komputer pula adalah salah satu lagi penyumbang utama hingga mengakibatkan kerugian, dengan jumlah taksiran dianggarkan mengjangkau sehingga RM 298,000.00. Selain ancaman itu, kebanyakan yang diajukan soalan survei turut mengakui sistem rangkaian komputer milik mereka tidak lepas dari tindakan penggodam yang menyerang sistem komputer atau sistem rangkaian komputer. Manakala kerugian yang lain pula disebabkan salahguna komputer oleh kakitangan sesebuah organisasi.

---

[55] Ringkasan hasil kaji selidik NISER – *ICT Security Survey for Malaysia 2000/2001* di sertakan dalam bahagian Lampiran VII

[56] Berdasarkan kepada survei yang dijalankan ke atas 113 organisasi memberi pandangan, 47% mengakui masalah yang dihadapi oleh mereka.

[57] Adalah dipercayai jumlah kerugian yang sebenar adalah lebih tinggi dari anggaran yang dikemukakan kerana kesukaran untuk menilai kerugian sebenar dari segi kos memulihkan 'kerosakan', memperolehi semula kehilangan operasi dan data serta kerugian sewaktu *'downtime'* – Rujuk laporan survei NISER di bahagian Lampiran

Selain dari kewujudan NISER, kerajaan Malaysia turut menubuhkan **Bahagian Keselamatan IT** pada 1hb Januari 2000. Peranan utamanya ialah untuk mengemukakan satu kerangka-kerja bagi mengimplementasikan polisi yang berkaitan dengan ICT dan keselamatannya bagi kegunaan semua agensi dan organisasi kerajaan. Pada masa yang sama, usaha yang bersungguh-sungguh turut dilakukan terutama dari segi penyediaan keperluan infrastuktur undang-undang yang lebih mantap dalam menghadapi dan menangani ancaman e-jenayah yang kini telah menjadi salah satu agenda penting negara selaras dengan kehendak pembangunan negara melalui prasarana ICT. Atas dasar itu undang-undang siber diperkenalkan, dengan tujuan menghadapi ancaman dan cabaran yang wujud, bersesuaian dengan situasi negara yang sedang beralih secara agresif ke era digital secara menyeluruh.

Kesemua langkah ini juga memperlihatkan sikap komited kerajaan menghadapi kemungkinan ancaman e-jenayah yang terbukti sedang pesat memuncak. Usaha-usaha ini sejajar dengan hasrat untuk menjadikan Malaysia sebagai hub rangkaian prasarana digital terpenting dan selamat di rantau Asia Tenggara sebagaimana yang digambarkan menerusi *Multimedia Super Corridor* yang terletak dalam lingkungan Putrajaya-Cyberjaya-Kuala Lumpur (KLCC) sejauh 50km. Begitu juga dengan penubuhan Suruhanjaya Komunikasi dan Multimedia (MCMC) yang dipertanggungjawab bagi mentadbirurus kegiatan yang berkaitan ICT negara.

BAB 6

6. Memerangi e-jenayah: Antarabangsa

Council of Europe yang telah mengambil satu resolusi yang dikenali sebagai *Convention on Cybercrime* telah mengemukakan definisi jenayah komputer dan jenayah yang berkaitan dengan komputer adalah seperti berikut;[58]

i) kesalahan yang dilakukan hingga mengakibatkan *confidentiality*, integriti dan *availability* sesuatu data dan sistem komputer yang melibatkan perlakuan mengakses, memintas, mengganggu gugat data, mengganggu gugat sistem dan menyalahgunakan perkakasan secara haram.

ii) kesalahan yang berkaitan dengan komputer seperti pemalsuan dan penipuan.

iii) kesalahan yang melibatkan kandungan sesuatu komputer atau sistem seperti pornografi dan pornografi kanak-kanak.

iv) kesalahan-kesalahan yang melibatkan hakcipta dan kesalahan yang berkaitan dengan hak-hak yang lain.

Di dalam konvensyen ini telah pun ditegaskan kesemua kesalahan yang disebut di atas mempunyai kaitan sama ada secara langsung dan tidak langsung dengan komputer dan sistem rangkaian komputer. Konvensyen ini juga menetapkan semua anggota *Council of Europe* akan mematuhi prosedur yang berkaitan dengan kuatkuasa, penyiasatan, pencarian dan proses memintas maklumat yang bertujuan untuk menjayakan penyiasatan. Dengan kata lain, ketetapan utama konvensyen ini ialah untuk mengadakan satu polisi bersama

[58] *European Treaty Series*. Number 185.

yang berkaitan dengan jenayah komputer yang boleh digunakan atau diambil sesuai mengikut ketetapan peraturan perundangan di samping untuk mengukuhkan kerjasama di peringkat antarabangsa[59].

Dari segi undang-undang, kesemua anggota *Council of Europe* telah bersetuju untuk bertindak secara bersama (dengan semua negara anggota) dan menerima resolusi konvensyen berkenaan. Tindakan ini merupakan satu usaha memerangi jenayah komputer dan jenayah yang berkaitan dengan komputer yang bertaraf antarabangsa sifatnya. Hal ini dibuktikan apabila kesemua ahli (negara) *Council of Europe* diminta untuk bekerjasama dengan menggunakan satu aplikasi yang serupa sebagai instrumen kerjasama antarabangsa untuk menangani permasalahan jenayah komputer.

Kerjasama dan ketetapan yang telah dipersetujui dibuat di bawah satu peraturan yang seragam dan boleh diaplikasikan mengikut kehendak dan peraturan atau undang-undang tempatan dalam konteks penyiasatan dan prosiding jenayah di mahklamah. Hal yang sama juga diapplikasikan bagi kesalahan-kesalahan jenayah yang berkait rapat dengan sistem komputer dan data atau untuk menghimpun dan mendokumentasikan keterangan bagi insiden-insiden jenayah yang berlaku secara elektronik. Pada masa yang sama, kesemua negara-negara ini bersetuju untuk menerima permintaan ekstradisi dari negara anggota yang lain, walaupun di antara kedua-dua negara berkenaan

---

[59] *European Treaty Series*. Number 185.

tidak memiliki perjanjian ekstradisi di antara mereka. Dengan kata lain, konvensyen ini akan digunakan sebagai asas perundangan di negara masing-masing untuk mengambil tindakan.

Kerajaan Amerika Syarikat pada masa ini turut mempertingkatkan kegiatan untuk mengesan perlakuan e-jenayah. Institusi penguatkuasa tempatan telah diberikan kuatkuasa undang-undang untuk melakukan penyiasatan termasuk melangkaui batas sempadan antarabangsa. Polisi yang dilakukan ini mempunyai tujuan mewujudkan rangkaian institusi di peringkat tempatan dan antarabangsa yang berkeupayaan untuk melakukan penyiasatan dan khususnya mewujudkan kerjasama[60].

Lebih-lebih lagi selepas insiden 11hb September 2001, kerjasama yang rapat di peringkat antarabangsa akan membolehkan usaha menghadapi ancaman jenayah dilakukan dengan lebih berkesan lagi. Terutama sekali pihak penguatkuasa di Amerika Syarikat berpendapat insiden ini mempunyai kaitan yang rapat dengan e-jenayah, walaupun peristiwa itu disifatkan sebagai tindakan terrorisme ke atas Amerika Syarikat. Justeru keperluan mewujudkan kerjasama antara negara di dunia adalah sebagai pendekatan yang terbaik bagi menghadapi perlakuan e-jenayah yang bersifat melangkaui batas sempadan (transborder crime). Maka, tidak hairanlah jika dikatakan negara negara lain

[60] Mitchele & Banker 1998 (Private Law Intrution, dalam Harvard Law Journal and Technology Vol 11, ms 699.

seperti Britain turut mengambil langkah pengawasan yang juga bersifat *transborders*[61]. Antara tindakan kerajaan Amerika Syarikat, ialah agensi perisikan seperti CIA menyediakan satu alat yang berkeupayaan melakukan analisis maklumat data elektronik yang dipintas[62] dengan tujuan mengesan kemungkinan ancaman yang bakal atau mungkin berlaku ke atas negara atau kepentingan Amerika Syarikat di luar negara. Kekuatan ini diperkukuhkan dengan kehadiran *Carnivorous* yang sedia terpasang di ibusawat-ibusawat telekomunikasi sama ada di dalam negara atau antarabangsa yang berperanan sebagai pengesan (sniffer) data elektonik yang bersifat 'mengancam'.

Di Eropah pula pengwujudan *Enfopol* bertujuan mengakses dan menganalisis mana-mana maklumat atau data elektronik yang dipintas dengan tujuan mengesan kemungkinan ancaman.

Satu lagi alat yang diwujudkan melalui kerjasama antara Amerika Syarikat, Britain, Canada, Australia dan New Zealand pula disebut sebagai *Echelon* yang memiliki keupayaan untuk memintas data elektronik sama ada dipancarkan melalui satelit atau pun kabel telekomunikasi atau medium lain yang digunakan untuk trafik data. Laporan yang dipetik dari *Interception Capabilities Report* (IC2000) yang dibentang di Parlimen Eropah, menyatakan bahawa alat yang kompleks dan canggih ini mampu menjalankan pengawasan

---

[61] The Sunday Times, 30th April 2000
[62] Denning,Dorothy (1997) "Cases involving Encryption in Crime & Terrorism"

maklumat elektronik sekurang-kurangnya dari 120 satelit (pengumpulan data) dan ibusawat kabel telekomunikasi darat dan di dasar laut.

BAB 7

7. Kesimpulan

Alam siber yang wujud pada masa kini terdapat di mana-mana. Analogi ini membawa pengertian bahawa ancaman jenayah siber juga berada di setiap penjuru. Lantaran itu perlakuan e-jenayah dari tindakan menyebar virus atau kod jahat sehingga kepada tindakan penyebaran bahan pornografi juga akan tetap berlaku selagi Internet boleh diakses secara global. Oleh itu setiap pengguna dan pihak penguatkuasa perlu pantas dan cekap untuk menghadapi ancaman seumpama ini. Aplikasi menangani jenayah secara konvensional diakui tidak lagi sesuai dan berkeupayaan. Justeru usaha untuk menyiasat dan mendakwa pesalah-pesalah e-jenayah bukanlah satu perkara mudah dan boleh dianggap enteng. Tidak ada satupun kaedah yang mudah dan efektif dalam menghadapi keseluruhan ancaman jenayah bentuk ini. Sebaliknya setiap satu perlu ditangani mengikut keperluan dan kehendak semasa.

Lebih-lebih lagi apabila jenayah komputer dan jenayah yang berkaitan dengan komputer yang terhad mengikut batas persempadanan fizikal geografi atau politik yang sedia ada. Maka amat perlu diwujudkan satu usaha yang bersepadu dan kerjasama yang melewati batas sempadan konvensional sama ada geografi atau politik sesuatu negara. Walau bagaimanapun, untuk menyempurnakan langkah ini bukanlah satu perkara yang mudah dan senang

dilaksanakan, terutama sekali apabila didapati undang-undang di antara negara yang sedia ada bukan sahaja tidak serupa tetapi tidak efektif apabila menjangkau batas sempadan geo-politik.

Sebagai contoh, apabila berlaku insiden menggodam di sesebuah negara dan serangan itu dilakukan dari negara yang lain, maka undang-undang yang wujud di negara mangsa sudah tentu tidak mempunyai jurisdiksi di negara di mana serangan dilancarkan. Keadaan akan bertambah sulit apabila negara tempat penggodam berlindung tidak menganggap perbuatannya sebagai satu jenayah. Ternyata undang-undang konvensional tidak efektif dari segi jurisdiksinya. Tambahan pula apabila maklumat yang diperlukan untuk bahan bukti berada di luar negara maka keadaan akan menjadi bertambah sulit.

Maka tanpa satu kerjasama yang baik atau persefahaman dari segi undang-undang, sudah pasti tindakan undang-undang ke atas penggodam (hacker) berkenaan tidak akan dapat dikuatkuasakan. Oleh yang demikian sekadar mempunyai undang-undang siber di sesuatu negara adalah tidak memadai jika proses penguatkuasaan tidak dapat dilakukan. Ini bermakna menyediakan sesuatu undang-undang (siber) hanyalah sebahagian daripada jalan penyelesaian. Sungguhpun begitu, tidak wajar pula jika tiada tindakan undang-undang yang khusus disediakan untuk menangani insiden seumpama ini.

Sungguhpun wujud halangan berpunca daripada perlakuan jenayah rentas sempadan sifatnya, tidak bermakna sesebuah negara harus berdiam diri dan membiarkan dirinya terus menjadi mangsa kepada penjenayah elektronik. Sebaliknya, usaha yang bersungguh-sungguh hendaklah sentiasa dipertingkatkan. Terutama sekali dengan menyediakan latihan dan usaha-usaha lain untuk mempertingkatkan tahap kecekapan supaya keupayaan menjalankan siasatan dan pendakwaan akan sentiasa dapat dijayakan. Hanya dengan mempertingkatkan pengetahuan di bidang berkaitan dan pelan tindakan yang pro-aktif akan dapat mempastikan setiap tindakbalas ke atas pelaku e-jenayah dijayakan dengan baik. Dengan itu, segala perkara yang berbangkit berkaitan ancaman e-jenayah di alaf ini akan dapat dibendung atau dikawal dengan cara membawa pelaku e-jenayah ke muka pengadilan. Hal ini akan memberi jaminan agar kawalan e-jenayah di negara ini akan dapat ditangani dengan lebih efektif, bukan hanya setakat bergantung kepada kewujudan undang-undang yang 'berbisa' semata-mata. Di samping itu kewajaran menyediakan instrumen undang-undang tidak kurang penting untuk menghadapi ancaman e-jenayah, setidak-tidaknya untuk memberi keyakinan kepada semua pihak bahawa Malaysia adalah sebuah negara yang tegas bagi menghadapi ancaman e-jenayah.

BIBLIOGRAFI

_____ (2001) *Prosecuting Cases That Involve Computers: A Resource for State and Local Prosecutors,* National White Collar Crime Center, 2001. (See also http://www.nctp.org and http://www.training.nw3c.org for information).

_____ (2001) *European Treaty Series – No. 185 on* 23rd November 2001.

_____ (2000) *"Assembly Condemns Misuse Of Information Technologies For Criminal Purposes,"* United Nation GA/9842 – 4th December 2000.

Bernama News Agency

Casey, Eoghan. (2000). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* San Diego: Academic Press.

Cheswick, William R. and Steven M. Bellovin. (1994) *Firewalls and Internet Security: Repelling the Wily Hacker.* Boston, Massachusetts: Addison-Wesley.

Computer Crime Act 1997

David S Wall, (2000) *"On the Politics of Policing the Internet: Striking the Right Balance"*, BILETA Computers and Law Conference.

Deloitte, Haskins & Sells. (1989). *Computer Viruses:* Proceedings of an Invitational Symposium, October 10–11, 1988. New York: Deloitte, Haskins & Sells.

Denning, Dorothy E. (1999) *Information Warfare and Security.* Boston, Massachusetts: Addison-Wesley.

Denning, D. and P. Denning. (1997) *Internet Besieged: Countering Cyberspace* Scofflaws. New York: Addison-Wesley.

Dorothy Denning, (1997) *"Cases Involving Encryption in Crime and Terrorism"* Scofflaws. New York: Addison-Wesley.

Evidence (Amendment) Act 1993 (A851).

Guisnel, Jean. (1997) *Cyberwars: Espionage on the Internet.* New York: Plenum Press, 1997.

McClure, Stuart, Joel Scambray, and George Kurtz. (1999) *Hacking Exposed.* Berkeley, California: Osborne/McGraw-Hill.

Mitchell & Banker, (1998) *"Private Law Intrusion"*, in Harvard Law Journal & Technology, Vol.11, Pg. 699.

National Institute of Justice. (2000) *Crime Scene Investigation: A Guide for Law Enforcement.* Washington, D.C.: U.S. Department of Justice, National Institute of Justice,. NCJ 178280.

Meinel, Carolyn P. (1998) *The Happy Hacker, Second Edition.* Show Low, Arizona: American Eagle Publications, Inc.

National Research Council. (1991) *Computers at Risk: Safe Computing in the Information Age.* Washington, D.C.: National Academy Press.

Rosenoer, Jonathan. (1997) *CyberLaw: The Law of the Internet.* New York: Springer.

Blacharski, Dan. (1998) *Network Security in a Mixed Environment.* Foster City, California: IDG Books,

Cohen, Frederick B. A.,(1994) *Short Course on Computer Viruses.* Somerset, New Jersey: John Wiley & Sons.

Davis, William S. (1991) *Computing Fundamentals: Concepts,* Third Edition. Boston, Massachusetts: Addison-Wesley Publishing Co., .

Deffie, Whitfield and Susan Landau. (1998) *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, Massachusetts: MIT Press.

Fiery, Dennis. (1994) *Secrets of a Super Hacker.* Port Townsend, Washington: Loompanics Unlimited.

Ford, Merilee, H. Kim Lew, Steve Spanier, and Tim Stevenson. (1997) *Internetworking Technologies Handbook.* Indianapolis, Indiana: New Riders Publishing.

Garfinkel, Simson and Gene Spafford. (1996) *Practical UNIX & Internet Security,* Second Edition. Sebastopol, California: O'Reilly & Associates, Inc.

Garfinkel, Simson and Gene Spafford. (1997) *Web Security & Commerce.* Sebastopol, California: O'Reilly & Associates, Inc., .

Hafner, Katie and John Markoff. (1995) *Cyberpunk.* New York: Simon & Schuster, Inc.

Landreth, Bill. (1989) *Out of the Inner Circle.* Redmond, Washington:Tempus Books of Microsoft Press.

Levin, Richard B. (1990) *The Computer Virus Handbook.* Berkeley, California: Osborne/McGraw-Hill.

Ludwig, Mark. (1998) *The Giant Black Book of Computer Viruses*, Second Edition. Show Low, Arizona: American Eagle Publications, Inc.

Martin, Fredrick T. (1998) *Top Secret Intranet.* Old Tappan, New Jersey: Prentice Hall PTR.

McCarthy, Linda. (1998) *Intranet Security.* Palo Alto, California: Sun Microsystems Press.

National White Collar Crime Center. (1999) *Using the Internet as an Investigative Tool,* First Edition. Fairmont, West Virginia: National White Collar Crime Center.

NISER ICT Security Survey for Malaysia 2000/2001

Northcutt, Stephen. (1999) *Network Intrusion Detection: An Analyst's Handbook.* Indianapolis, Indiana: New Riders Publishing.

Olson-Raymer, Gayle. (1996) *Terrorism: A Historical & Contemporary Perspective.* New York: American Heritage Custom Publishing.

Parker, Donn B. (1983) *Fighting Computer Crime.* New York: Scribners.

Parker, Donn B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information.* New York: John Wiley & Sons, Inc.

Parsaye, Kamran and Mark Chignell. (1988) *Expert Systems for Experts.* New York: John Wiley & Sons, Inc.

Pipkin, Donald L. (1997) *Halting the Hacker: A Practical Guide to Computer Security.* Upper Saddle River, New Jersey: Prentice Hall.

Raymond, Eric S. (1998) The New Hacker's Dictionary, Third Edition. London, England: MIT Press.

Robbins, Arnold. (1999) *UNIX in a Nutshell*, Third Edition. Sebastopol, California: O'Reilly and Associates, Inc.

Rodgers, Ulka. (1991) *ORACLE: A Database Developer's Guide.* Upper Saddle River, New Jersey: Yourdon Press.

Rosenblatt, Kenneth S. (1996) *High-Technology Crime: Investigating Cases Involving Computers.* San Jose, California: KSK Publications.

Russell, Deborah and G.T. Gangemi, Sr. (1992) *Computer Security Basics.* Sebastopol, California: O'Reilly & Associates, Inc.

Schulman, Mark. (1992) *Introduction to UNIX.* Indianapolis, Indiana: Que Corporation.

Schwartau, Winn. (1995) *Information Warfare: Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press.

Shimomura, Tsutomu and John Markoff. (1996) *Take-Down.* New York: Hyperion.

Slatalla, Michelle and Joshua Quittner. (1995) *The Gang That Ruled Cyberspace.* New York: Harper Collins.

Sterling, Bruce. (1993) *The Hacker Crackdown.* New York: Bantam Books.

Stoll, Cliff. (1989) *The Cuckoo's Egg.* New York: Simon & Schuster, Inc.

Strassmann, Paul A. (1995) *The Politics of Information Management Policy Guidelines.* New Canaan, Connecticut: The Information Economic Press.

Tittel, Ed and Margaret Robbins. (1994) *Network Design Essentials.* Boston, Massachusetts: Academic Press, Inc.

Trippi, Robert R., and Efraim Turban. (1993) *Neutral Networks in Finance and Investing.* Cambridge, England: Probus Publishing Co.

U.S. Department of Justice, (2001) *Computer Crime and Intellectual Property Section. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Washington, D.C.: U.S. Department of Justice, Computer Crime and Intellectual Property Section.

Wang, Wallace. (1998) *Steal This Computer Book.* San Francisco, California: No Starch Press.

Wolff, Michael. (1996) *How You Can Access the Facts and Cover Your Tracks Using the Internet and Online Services.* New York: Wolff New Media, LLC.

Web Sites

Computer Crime and Intellectual Property Section of the U.S. Department of Justice, http://www.cybercrime.gov.

MyCERT: http://www.mycert.org.my

NISER: http://www.niser.org.my

National Cybercrime Training Partnership, 877–628–7674, http://www.nctp.org.

Infobin, (1998). *Anonymous. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, Second Edition. Indianapolis, Indiana: Sams, 1998. http://www.infobin.org/cfid/isplist.htm

The Internet Watch Foundation (IWF) http://www.iwf.org.uk/about/index.htm

OECD, Organisation for Economic Co-operation and Development: an international organisation helping governments tackles the economic, social and governance challenges of a globalize economy. http://www.oecd.org/

Ipsos-Reid website http://www.angusreid.com/latest.cfm

Lampiran

Lampiran I

Print and fax it to MyCERT at 603 - 89960827

General Information

1 Incident number (to be assigned by MyCERT).....
2 Reporting site information
2.1 Name of Organization... .....
2.2 Name of Domain (e.g., mycert.mimos.my).....

Contact Information

1 Your contact information
1.1 Name.....
1.2 E-mail address.....
1.3 Telephone number.....
1.4 FAX number.....

Incident Categories

1 Please indicate the incident catagories
1.1 Nework Abuse
1.1.1 Intrusion.....
1.1.2 Destruction.....
1.1.3 Denial of service attack.....
1.1.4 Hack Threat.....
1.1.5 Probe/Scan.....
1.1.6 Spoofing..... .....
1.2 Email Abuse (please provide the full header)
1.1.1 Mailbomb.....
1.1.2 Virus.....
1.1.3 Email Forgery.....
1.1.4 Harrassment.....
1.1.5 Spamming.....
1.1.6 Others.....(please specify):.....

Detail description of the incident

1 Please complete in as much detail as possible
1.1 Suspected date and time of attack.....
1.2 Suspected method of intrusion (e.g., name of virus, name of exploit script, etc.).....
1.3 How you discovered the incident.....
1.4 The source of the attack (if known).....
1.5 Steps taken to address the incident (e.g., binaries reinstalled, patches applied).....
1.6 Planned steps to address the incident (if any).....
2 Please append any log information or directory listings

and time zone information relative to GMT to the end of this document.....

Other information

1 What assistance would you like from MyCERT.....
2 Would you allow MyCERT to reveal your contact info.....
3 Any additional information.....

Lampiran II

Denial Of Service Attack

Denial Of Service Attack, the most recent Internet Plague, is giving dramatic effects on the service and stability of its victims. Although this is not something new, the increased accessibility of the Internet and the ever-decreasing age and sophistication of the average computer hacker, is resulting in an enormous surge in the type of attack which is specifically and solely intended to deny service to the system or application. In many cases, the exploit code to conduct these attacks are freely available on the Internet, and it can affect the stability of the system only by a few keystrokes and by mere click of the mouse. These attacks take advantage of the deficiencies in the TCP/IP protocol, which is used as the baseline for communications on the Internet, and they are difficult, if not impossible, to trace their source since the packets can be "spoofed" or "forged" as they come from any source on the Internet.

Several types of attacks:
SYN ATTACK

PROBLEM:

All systems on the Internet, which accept TCP connections, are susceptible to a SYN attack.

From CERT Alert CA-96.21:

When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections--telnet, Web, email, etc.

The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server. Here is a view of this message flow:

```
Client          Server
------          ------
SYN---------------->

<----------------SYN-ACK

ACK---------------->
```

Client and server can now send service-specific data.

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection. The server has built in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the victim server system; these appear to be legitimate but in fact reference a client system that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the victim server system.

The half-open connections data structure on the victim server system will eventually fill; then the system will be unable to accept any new incoming connections until the table is emptied out. Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim server system will recover. However, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can expire the pending connections.

In most cases, the victim of such an attack will have difficulty in accepting any new incoming network connection. In these cases, the attack does not affect existing incoming connections nor the ability to originate outgoing network connections. However, in some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative. The location of the attacking system is obscured because the source addresses in the SYN packets are often implausible. When the packet arrives at the victim server system, there is no way to determine its true source. Since the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering..."

SOLUTIONS:

The SYN Attack rests at the very core of identified weakness of the TCP/IP protocal, and are difficult, if not impossible in some cases, to correct.

Things you can do:

Deploy System Operating Patches

Several vendors have released operating system patches to compensate and react to SYN attacks. Check with your operating system vendor(s) to ensure you have patched, at least, your publicly available sites.

Deploy Monitoring Systems

Several Intrusion Detection Systems now look for SYN attacks. Ensure you have a monitoring and reporting procedure in place. Some vendors that sell SYN based detectors such as:

ISS:
http://www.iss.net/RealSecure

Checkpoint:
http://www.checkpoint.com/fw21/syndefender/index.html

Report abuse to your Internet Service Provider

When a Denial Of Service attack is detected on your systems, contact the Security Department of your Internet Service Provider to have them assist in tracking down the source of the active attack.

More information on the SYN attack and its background can be obtained from:

http://www.fc.net/phrack/files/p48/p48-13.html

- ICMP or PING FLOOD ATTACK

PROBLEM:

Unauthorized users can disrupt your service or consume your available network bandwidth by sending a constant stream of forged ICMP packets to your system(s).

Known as a "Ping Flood" attack, computer hackers send steady stream of PING packets (known as "echo request" packets) to your system(s). In many cases, this flood of traffic can consume system resources, and even consume significant amounts of bandwidth on mid to low speed connections (eg; T1 and below).

SOLUTIONS:

- ***Block Traffic*** In most cases, you can simply deny ICMP packets on your network firewalls to prevent the traffic from affecting your systems. However, since the traffic is still traversing your access line, you need to ensure your Internet Service Provider is involved.

- ***Report abuse to your Internet Service Provider***

  When a Denial Of Service attack is detected on your systems, contact the Security Department of your Internet Service Provider to have them assist in tracking down the source of the active attack.

- MAIL BOMB

PROBLEM:

Unauthorized users can send large amounts of large email messages to and through your email server, often filling up disk space on your mail system, denying email services to other users.

These attacks usually involve the unauthorized user(s) sending thousands of large binary attachments to a single or multiple valid users on your server (or spooling through your server in attack against someone else, using your server to hide his tracks). Once the disk fills up, the server rejects additional messages.

SOLUTIONS:

- ***Deploy monitoring systems***

Ensure your monitoring systems monitor the number of messages coming into your server, and reporting sudden spikes in traffic.

In addition, monitoring systems should check for active disk space on your systems, and reporting when your partitions are in jeopardy.

- ***Ensure mail spool areas are on large, dedicated disk partitions***

Ensure that your mail spool and log directories would not affect other aspects of the system if they were filled.

For example, having the mail spool, queue and/or users mail directories on a Unix ROOT file system may affect the availability of the system itself if the system was subject to a successful Denial Of Service Attack.

- ***Report abuse to your Internet Service Provider***

When a Denial Of Service attack is detected on your systems, contact the Security Department of your Internet Service Provider to have them assist in tracking down the source of the active attack.

SYSLOG and SNMP Bombs

PROBLEM:

This issue is more like the MAIL BOMB ATTACK.

Unauthorized users can send large amounts of large log messages to your logging server, often filling up disk space on you system, denying collection of additional logging data.

These attacks usually involve the unauthorized user(s) sending thousands of large log messages to your server.

Once the disk fills up, the server rejects additional messages.

SOLUTIONS:

- ***Deploy monitoring systems***

Ensure your monitoring systems monitor the number of log messages coming into your server, and reporting sudden spikes in traffic.

In addition, monitoring systems should check for active disk space on your systems, and reporting when your partitions are in jeopardy.

- ***Ensure log directories are on dedicated disk partitions***

Ensure that your mail spool and log directories would not affect other aspects of the system if they where filled.

For example, having a log message directory on a Unix ROOT file system may affect the availability of the system itself if the system was subject to a successful Denial Of Service Attack.

- ***Report abuse to your Internet Service Provider***

  When a Denial Of Service attack is detected on your systems, contact the Security Department of your Internet Service Provider to have them assist in tracking down the source of the active attack.

- SMURF ATTACK

PROBLEM:

As explained at http://www.quadrunner.com/~chuegen/smurf.cgi :

The "smurf" attack, named after its exploit program, is one of the most recent in the category of network-level attacks against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of them having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function noted below, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could be potentially hundreds of machines reply to each packet.

The "smurf" attack's cousin is called "fraggle", which uses UDP echo packets in the same fashion as the ICMP echo packets; it is a simple re-write of "smurf". Currently, the providers/machines most commonly hit are IRC servers and their providers. There are two parties whom are hurt by this attack... the intermediary (broadcast) devices--let's call them "amplifiers", and the spoofed address target, or the "victim". The victim is the target of a large amount of traffic that the amplifiers generate.

Let's look at the scenario to paint a picture of the dangerous nature of this attack. Assume a co-location switched network with 100 hosts, and that the attacker has a T1. The attacker sends, say, a 768kb/s stream of ICMP echo (ping) packets, with a spoofed source address of the victim, to the broadcast address of the "bounce site". These ping packets hit the bounce site's broadcast network of 100 hosts; each of them takes the packet and responds to it, creating 100 ping replies out-bound. If you multiply the bandwidth, you'll see that 76.8 Mbps is used outbound from the "bounce site" after the traffic is multiplied. This is then sent to the victim (the spoofed source of the originating packets).

SOLUTIONS:

- ***Apply filtering rules at your border router.***

  Filter out ICMP/UDP packets directed for broadcast addresses. To filter out ICMP directed broadcast, please use this vendor specific information (for others please refer to http://www.quadrunner.com/~chuegen/smurf.cgi):

- Cisco - as of IOS version 12.0, a feature called no ip directed-broadcast" is now the default configuration. For previous versions of IOS, use the interface configuration command to enable this.
- Bay Networks - You can use this command

```
[1:1]$bcc
bcc> config
hostname# ip
ip# directed-bcast disabled
ip# exit
```

- 3Com NetBuilder - To disable 3Com routers from forwarding directed broadcast, you can enter this command

SETDefault -IP CONTrol = NoFwdSubnetBcast

- ***Apply patches for hosts to discard ICMP directed broadcast***

Here is the relevant information for specific platforms:

- IBM AIX 4.x - use this command

```
no -o bcastping=0        # disable bcast ping responses (default)
```

- Solaris - add this command into /etc/rc2.d/S69inet

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

- FreeBSD - as of version 2.2.5, FreeBSD does not respond to echo request directed for broadcast addresses. The relevant sysctl parameter is

```
net.inet.icmp.bmcastecho
```

- NetBSD/OpenBSD - use this parameter for sysctl

```
sysctl -w net.inet.ip.directed-broadcast=0
```

- Linux - in Linux you can completely deny echo request by compiling this option in the kernel, i.e. CONFIG_IP_IGNORE_ECHO_REQUESTS.

  However, this violates RFC 1122. To protect Linux hosts from this attack, one can make use of Linux's in-kernel firewall capability. This can be done with

```
ipfwadm -I -a deny -P icmp -D 123.123.123.0 -S 0/0 0 8
ipfwadm -I -a deny -P icmp -D 123.123.123.255 -S 0/0 0 8
```

  (replace 123.123.123.0 and 123.123.123.255 with your base network number and broadcast address, respectively).

Lampiran III

DESTRUCTION

Destruction is defined as attempts made to destroy the system, data/information and/or physical assets, basically efforts made to cripple the operations of a network. Such cases generally begins with a repeated attempts using various security tools or methods which can be obtained via searching through Internet or by just asking through newsgroup or more commonly, "chatting". Once the attempts are successful, then the possibility of the network being terrorised will definitely be achieved.

For example by:

- inserting a logic bomb, virus or worm into a program to cause loss of data on a disk and impair operations.

  logic bomb
  an application or system virus designed to "explode" or execute at a specified date and time.

  virus
  a program that attaches itself to other programs, be it a document, system or application virus.

  worm
  an independent program that replicates its own program files until it destroys other systems/programs or interrupts operation of networks or computer system,

- monopolize the available space in memory or a system library, or unauthorized modification of a password to a file or a system rendering them inaccessible.

Perhaps the question that should have been asked is the reason behind the so-called "attempts", which resulted to the crippling of the company's network. Below are some of the examples. \

- INTERNAL EXPLOITATION
  Problem:
  Malicious user whose sole purpose is to hurt the targeted network eg. ex- or dissatisfied employees who already knows the company secrets and knows exactly which target to hit.

  Solutions:

  - Any organizations must update user database to ensure all ex-employees' have been deleted.
  - Organizations must change all important passwords especially the root as soon as system administrators or any previlege users leave the company.
  - Watch for disgruntled employees and resolve problems before they escalate.

  Problem:
  Intentional user whose purpose is to gain something which is useful to them eg. foreign employees who already have access to computers, networks, the company site and many other

resources they may need; sabotage the system and assigned password for all access to the system including the hardware; and finally ask for a large sum of money in return for the passwords.

Solutions:

- There should be at least two people in charge of the system and the network. The exact number of people needed depends on the size of the system and the network of the organization. Ensure sufficient backup in human resources.
- Always create a back up for your system and most importantly your customer data. This will enhance customers' trust and confidence in the organization.
- Try to create a knowledge sharing environment or transfer of technology session within the organization.

- EXTERNAL EXPLOITATION

Problem :

Industrial spies poses as a legitimate person in the organization and tricks users into giving information. This can occur through phone calls, forged E-mail messages, or even in-person visits to the business site. This technique requires extensive research, but is usually very successful.

Solution:

- Create a good company policy on social security which includes physical security and barriers, installed, at business site, the kind of things a representatives should be allowed to say over the phone and shredding or incinerating potentially sensitive documents.

Problem:

Crackers/hackers using variety of tools and techniques to gain access to computers over the Internet just for "kicks".

Solution:

- Build a secure network and maintain the system security by keeping it up to date ie monitor access and use via event logging, monitoring system, clock synchronization etc.
- Always be informed on latest bugs or security holes in network or operating system software. Install patches as soon as they become available.
- Keep abreast on security tools development.

Lampiran IV

Intrusion

It is in which attempts made for unauthorized access to a system with the purpose of simply to test the security of the network, use the facility as a launching pad for further attacks on other systems, to modify information or to steal information, etc.

Problem: Intrusion is committed by gaining initial access to a particular host by discovering a password for a user account on the system. The intruders will then attempt to become root on the compromised system. Intruders are actually committing the following activities:

1. Sniffer Attacks- capturing data as it traverses the net
2. E-mail attacks- gaining system access through vulnerabilities in network service software
3. Network File System attacks- gaining data access through vulnerabilities in operating system software
4. Network Infrastructure attacks- denial of service through attacks on routers and name servers, i.e. for purpose of impersonating the server
5. IP spoofing attacks- gaining system access by tunneling through firewalls
6. WWW threats- gaining users or system information through the web or cgi programs.

Solutions:

A . Report the intrusion to your Internet Service Provider

The report should include the following:

1. The originating IP address
2. Timestamp with the exact time zone, i.e. GMT, PDT, MYT
3. Brief description on the method used in the activity

B. Check your systems for signs of intrusion due to this incident.

1. Check the su, ftpd, and ftp binaries (for example, "/bin/su", "/usr/ucb/ftp" and "/usr/etc/in.ftpd" on Sun systems) against copies from distribution media.
2. Check for the presence of any of the following files:
   "/usr/etc/..." (dot dot dot), "/var/crash/..." (dot dot dot),
   "/usr/etc/.getwd", "/var/crash/.getwd", or
   "/usr/kvm/..." (dot dot dot).
3. Check for the presence of "+" in the "/etc/hosts.equiv" file.
4. Check the home directory for each entry in the "/etc/passwd" file for the presence of a ".rhosts" file containing "+ +" (plus space plus).
5. Search the system for the presence of the following set-uid root files: "wtrunc" and ". a".
6. Check for the presence of the set-uid root file "/usr/lib/lpx".
7. You may refer to the following URL for further intrusion detection checklist:
   ftp://ftp.cert.org/pub/tech tips/intruder detection checklist

C. Take the following steps to secure your systems.

1. Save copies of the identified files to removable media
2. Replace any modified binaries with copies from distribution media
3. Remove the "+" entry from the "/etc/hosts.equiv" file and the "+ +" (plus space plus) entry from any ".rhosts" files.
4. Remove any of the set-uid root files that you find, which are mentioned in A5 or A6 above.
5. Change every password on the system.
6. Inspect the files mentioned in A2 above for references to other hosts.
7. You may also go the following site for further information on steps for
8. recovering from a UNIX root compromise:

ftp://infor.cert.org/pub/tech tips/root compromise

Lampiran V

Fraud

It is strictly where a computer system is *instrumental to the crime*, for example, it's processing capability is used to divert funds illicitly.

Types of fraud:

1) E-mail forgery/user impersonation
2) Electronic commerce
   *Payment Anonymity – untraceable, i.e. Digital Cash (a new 'net currency')
   *Illegal transaction – funds transfer
   *Intermediation Server vulnerabilities or loop-holes
3) Electronic Banking
   *ATM and credit card fraud
   *Internal personnel fraudster

Where The Frauds Are

Internet Scam

The twelve scams most likely to arrive via bulk email in consumers' email boxes:

1. Business opportunities scams: These offers make it sound like it is very easy to start a business that will earn piles of money without much work, selling or cash. Many of these "opportunities" are actually illegal pyramid schemes that are masquerading as legitimate opportunities to earn money.
2. Make money by sending bulk email: These solicitations offer to sell you bulk email lists (consisting of millions of email addresses), spam software (usually very poor in quality), or services to send spam on your behalf. Don't do this.
3. Chain letters. No list of scams would be complete without this old "favorite" - email style. Here you're asked to send a small amount of money (or some item) to each of four or five names at the top of the list, and then forward the message including your name at the bottom, via bulk email. Many of these letters claim they are legal chain letters loses money. Even if there is a "product" such as a report on how to make money, it does not make these schemes they are not. Further, nearly everyone who participates in these legal.
4. Work-at-home-schemes. The most common work-at-home scam promises that you'll earn money for stuffing envelopes. For example, you're promised you'll earn $2.00 for every envelope you stuff. In fact, there never is any real envelope stuffing employment available. Instead, you pay to register and then you're instructed to send the same envelope-stuffing ad via bulk email to others. The only money you can earn would come from others who fall for the scam and pay to register. Finally, if you did actually do work for one of these outfits (for example, some promise to pay you for craft work), they'd refuse to pay you and say your work didn't measure up to their "quality standards."
5. Health and diet scams. These are similar to the miracle cures offered off-line: ways to lose weight without eating less or exercising, "scientific breakthroughs," "secret formulas" which provide cures for hair loss, and herbal formulas that liquify fat cells so that they are absorbed by your body. These scams often include testimonials from "famous" medical experts you haven't heard of. Of course, these gimmicks don't work.

6. Effortless income. The newest version offers get-rich-quick schemes to make unlimited profits exchanging money on the world currency markets. There are lots of variants, but they all promise vast riches with no work. Beware of these scams.
7. Free goods. These offers promise expensive items such as computers... for free. They ask you to pay a fee to join, and then you have to bring in a certain number of other members. Many of these scams are just disguised pyramid schemes.
8. Investment opportunities. These scams promise outrageously high returns... and of course, there is "no risk." Many of these scams are illegal schemes, in which early investors are paid with the money from later investors. This gives the early investors the illusion that the system works and they are then encouraged to invest more money (which they eventually lose). The sales pitches for these offers include claims of high-level financial connections, that the promoters are privy to inside information, or promises that they'll guarantee the investment. The promoters are long gone if you try to take advantage of their "guarantees."
9. Cable descrambler kits. These scams offer kits or information on how to receive cable transmissions without paying any subscription fees. There are two problems with these offers:
    1) the kits and information don't work; and
    2) even if they did work, it is illegal to steal service from cable television companies.

    (Further, many cable companies have aggressively been prosecuting cable service theft.)

10. Guaranteed loans or credit, or easy terms scams. There are lots of variants of this scam: home equity loans that don't require any equity in your home, loans regardless of your credit history, offshore bank loans, credit cards regardless of your credit history, etc. Sometimes these offers are combined with pyramid schemes that offer to pay you for attracting other participants to the scheme. However, they are scams - the loans don't come through, you are turned down unless you meet stringent requirements, or the credit cards simply don't arrive.
11. Credit repair scams. These scams promise to erase accurate negative information from your credit file so that you can now qualify for loans, mortgages, or credit cards. The promoters of these scams cannot deliver. Further, if you follow their advice and lie on a loan or credit application, misrepresent your Social Security number, or get an Employer Identification number from the Internal Revenue Service under false pretenses, you will be committing fraud and violating federal laws. Don't fall for this scam.
12. Vacation prize promotions. Last, but not least, is a scam in which you receive electronic verification congratulating you because you've "won" a fabulous vacation, or you've been "specially selected" for this opportunity. The "deluxe cruise ship" may well be more like a tugboat, upgrades can be very expensive, and hotel accommodations are likely to be very shabby.

How To Avoid Scam

1. Always use common sense. If you have a gut feeling that something isn't legitimate, you're probably right and just avoid it.
2. Make sure the company has a phone number and physical address. Call the company back. Check with Information to see if the phone number actually belongs to that company.
3. Always ask for references and check them carefully. A reputable company will be pleased to send you additional information and give you as many references from satisfied customers as you want.
4. Do ask on-line promoters where their company is incorporated. If you're suspicious, call the state's secretary of state and ask if the company is incorporated with them and if it has a current annual report on file.
5. Check with ISPs to see if the company has a received a series of complaints.

6. Always make sure that you get a strong guarantee. Ask the company what will happen if you want to return the product or service. You might even ask for references of people who have returned the product and received refunds.
7. Avoid falling for high-pressure sales tactics. Scamsters always want your money right now. They don't want to give you time to think about your decision. If you are pressured to decide right now, decide "no."
8. Pay by credit card. That gives you recourse if you have a problem. If you pay by credit card and have a problem, you can call your bank and do a "charge back." What that means is that you have the credit card company "charge back" your purchase to the vendor and give you a credit. But do be careful giving out your credit card number (especially by email).
9. Don't respond to bulk emails. Be skeptical of offers that use LOTS OF CAPITAL LETTERS and punctuation!!! Emails that shout at you are often bogus, such as "Discover how you can make BIG $$$$$ MONEY in NO TIME AT ALL!!!!!
10. Always print a hard copy of any on-line offer that you're considering. Make sure you keep the email address, Internet address (URL), and any other information, as well as the date and time that you saw the offer. Save this information in case you need it later.
11. Beware of promoters who try to sell things using an anonymous email address such asnon12345@anon.company.com, user@domain.com or a post office box.
12. Don't participate in a pyramid scheme. If you are asked to send money to ten people, who each send money to ten other people, who then each send money to ten more people, etc., this is an illegal pyramid scheme. Don't do it.
13. If you're told that you have won a prize, be skeptical. If you are told you have won a prize and have to pay money, always refuse the prize.

Credit Card Fraud

There has been a great amount of publicity about the dangers of credit card fraud on the Net which makes consumers afraid to reveal their credit card numbers over the Net.

Therefore, online shoppers should take precautions when giving out any confidential information (including credit card number) over the Internet, over the phone or anywhere else for that matter. Always use common sense -- it is the best rule of thumb. There has been an increase in the number of merchants who have been scammed by crooks who place fraudulent orders using stolen credit card information. Unfortunately, merchants are not provided the same protection as consumers when it comes to credit card fraud. In fact, merchants are completely at risk.

It has been discovered that crooks can even now create fictitious credit card numbers based on the algorithms used to produce authentic numbers. These fictitious credit card numbers pass through verification and will be given approval codes. There are also newsgroups, which post stolen credit card data (so if your card number is stolen, it may be posted to the world in a matter of minutes).

Eight Steps to Minimise Credit Card Fraud

Below are some tips for merchants to minimize the risk of credit card fraud:

1. Begin taking a few extra steps to validate each order. Don't accept orders unless complete information is provided (including full address and phone number). Address Verification should be required for all credit card orders.

2. Be wary of orders with different "bill to" and "ship to" addresses. Anyone who uses a different "ship to" address should be required to send a fax with their signature and credit card number authorizing the transaction.
3. Be especially careful with orders that come from free email services -- there is a much higher incidence of fraud from these services (hotmail.com, juno.com, usa.net, etc.). Many businesses would not even accept orders that come through these free email accounts anymore. That's because it's so easy for a scamster to open a free, anonymous email account in another person's name and then send you, the merchant, an order using the fake email account and a fraudulent credit card number.
4. Be especially wary of orders that are larger than your typical order amount, and orders with next day delivery. Crooks do not care what it costs, since they aren't planning on paying for it anyway.
5. Pay extra attention to international orders. Do everything you can to validate the order before you ship your product to a different country. Do not ship international orders, which have different "bill to" and "ship to" addresses.
6. If you're suspicious, pick up the phone and call the customer to confirm the order and this will save you a lot of time, money, in the long run.
7. Consider using software or services to fight credit card fraud online. There are some positive reviews from those who have used Cybersource and Clear Commerce Corp.
8. If you (as a merchant) do have the misfortune of being scammed by a credit card thief, you should contact your merchant processor immediately or your ISP and inform them of the situation.

E-mail Spams

As "spam" is cheap and easy to create, fraudsters increasingly use it to find investors for bogus investment scheme or to spread false information about a company. Spam allows fraudsters to target many more potential investors than cold calling or mass mailing. Spammers actually can send personalized messages to thousands and even millions of Internet users at a time by using a bulk e-mail program.

How To Reduce Spams

1. Always use a separate email address when you post to newsgroups and mailing lists and this email address should not be used for personal email. Then, you can quickly browse the email in this account to see what's spam and what isn't. And your main personal email address would not be as clogged with spam.
2. Do not buy anything from a company that spams or visit their sites and get more information. If you respond to their spams, you're encouraging them to continue spamming.

What to do if you get spammed?

1) Probably the most ineffective anti-spam technique is asking the spammer to stop. It virtually never works.

2) Complain to the ISP of the spammer.

3) If the spam includes a URL, like the "Bargains" spam, complain to the postmaster of that domain and to the ISP or company that hosts that domain. Often, the company will deny that they are even aware of the spam, which may or may not be true.

4) Complain to other relevant companies.

Lampiran VI

Theft

When we are talking about theft, we are not only expressing it in terms of stealing physical objects such as computers, modems, keyboards, chips, electronic devices etc, but broadly, it can also be defined as loss of data or files from your own workstation or worst, your server, either by remote or local tamperings, or by vandals.

Below are some examples of theft.

Data modifications:
The user accesses a file on a local or network drive, and modifies, deletes and overwrites it with new data. Sometimes, this is used to modify system settings or browser security settings.

Password theft:
The user steals a network or an Internet user name and password from the local machine or server. A third party can then used the password to access protected resources.

File theft:
The user steals a file from the local or network and sends it to an outside user via the open Internet connection. The user has root access to any file that the victim has right to.

There are two ways that can promote theft; one is called **remote accessing** and the other, known as **vandals**.

When a potential hacker has to acquire the user id and password of the targeted host to intrude the respective system, it is called **remote accessing**. The unauthorized information can be gained either by repeated attempts using security tools available via Internet, or by exploiting published vulnerabilities or bugs. Often, this is one of the initial steps, which leads to compromising a system.

To protect it from these unauthorized accesses, system administrators must always be aware of the latest bugs or security holes in network or operating system software. It is of utmost importance to have a routine check on the log files so that any further tampering on the system could be avoided.

Unlike remote accessing, **vandals,** (sometimes referred to as "hostile applets") are more malicious where it can execute automatically when a user views a web page, receives pushed contents, or opens an email messages, ie, the victims will not even aware that they are running the program. It can take in the form of hostile Java, ActiveX, JavaScript, VBScript, html (including booby trapped shortcuts), plug-ins, helper applications and pushed executables. Other than the three examples of theft mentioned above, vandals can also cause loss or denial of service within the local computer system. For example, they can flood the system with data so that it runs out of memory, or they can slow down Internet connections.

The best way to protect yourself against a hostile applet is to know who you are downloading a Web page from or who has sent you an HTML page as an e-mail attachment.